Tampa Bay Romance Scam

Part 1: Fraud Analysis

1. The other types of cyberfraud that may fall under this case scenario are phishing and identity theft. According to the textbook, phishing involves "sending fraudulent communications to obtain personal information" (Graham & Smith, 2024, p. 86). On the other hand, identity theft involves using another person's credentials in some way to deceive. In this case, David provided examples of both. To make himself look successful and wealthy to Jennifer, he took photos from an actual realtor's Instagram account and impersonated the user who owns the account. From Jennifer's perspective, this gave her the impression that he's a well-stabled man. This is one example of identity theft. Another example of identity theft is the use of stolen business information. David was able to forge a contractor's business credentials on an estimate to gain money for the "renovations" of their "property". In a typical phishing attack, attackers usually send legitimate-looking emails to gain trust and lure their victims into giving their credentials. If they succeeded by tricking the victim, this is followed by them clicking a link to a fake login webpage. Although David didn't use any emails to trick Jennifer, he used fake documents, such as fake tax returns and a "professional" looking business plan, to gain her trust. Another example of phishing is using video chats and phone calls to build trust before the execution of his plan.

David's motive behind this plan is primarily money seeking, with the assistance of personal information seeking. Every point of contact consisted of direct financial requests for a large amount of money. In the third month, he requested from Jennifer $40,000 for an estate "investment". In the fourth month, he requested $15,000 for a "renovation" to their "dream home". In the fifth month, he asked for her "investment" of $18,000 for the business partnership. Lastly, in the sixth month, before his plan was exposed, he asked for $8,500 for his "daughter's" medical emergency. From these short periods of transactions, David was able to gain a total of $81,500 from Jennifer. This led to Jennifer's loss of funds from her 401k, credit cards, and her bank account. In addition, he ran numerous scams on other victims and was a part of a fraud ring that included money mules. Money mules are individuals who transfer money to third parties for further transfers (Graham & Smith, 2024, p. 137). However, these back-to-back transactions wouldn't have been possible without personal information seeking. David had to gain Jennifer's trust for her to provide the money. To do so, he had to create false stories to get her to send money. How this case combines with romance and investment scams is that David used dating apps to target his victims and then build their trust by telling his dating life and giving them gifts. As for the investment scams, he impersonates an estate agent and creates fake business plans to lure his targets in on his requests or "investments".

2. The five red flags shown in this case are asking for a large amount of money when they have just met, they haven't met in person, the lovebombing, the payment methods, and the

investment pitch. All these transactions were made by them calling or texting each other, but not once have they seen each other in person or gone on dates. How he was able to manipulate Jennifer was by using emotional vulnerability, urgency, authority, false legitimacy, and guilt by creating false stories to create a sense of connection and trust with Jennifer. When they first met, he told a story about his "late wife" and told her how he was deeply interested in her. He also sent her gifts while they were "dating". This plan worked out great for David because Jennifer was divorced and was seeking another chance at love. Through this tactic, he was able to build an emotional bond with her. After two months, he had told her about the "one-in-a-lifetime" investment, and if they didn't get the auction, they would lose the property, which instantly put a sense of urgency on Jennifer. However, to gain Jennifer's attention and execute his plan, he had to present himself as an estate agent and entrepreneur. He showed this by presenting "business documents" and gifts from "his business". From his authority and false legitimacy, this gave the impression that he was trustworthy and serious. However, when Jennifer started to raise suspicions about the property, David instantly created a false story about his daughter's medical fees, which soon caused Jennifer to send money out of sympathy and guilt.

The technical elements in this case were the fake website, images, business documents, and other documents that David gathered and crafted. As for the social engineering elements, he used pain points, guilt, flattery, and false stories. How he was able to make these business documents and pictures very legitimate was by stealing other photos from the internet and stolen business credentials. Also, through research of Tampa Bay properties. Before attackers craft their bait, they do passive reconnaissance first to gain insight into how victims operate and communicate on a day-to-day basis. For companies, attackers study the internal communications sent between business personnel and employees and everything else about the company to get an idea of how to draft these emails, documents, and websites to trick their victims. These emails often include familiar terms that are expected from employees or individuals with minimal grammatical errors that are able to bypass the eyes when read. However, for this case, David utilized the information from a contractor and the Tampa Bay seal to make the documents seem legitimately sourced from the business. He also managed to use a real address from a property, although it was already sold. This makes the plan verifiable and realistic.

3. Jennifer was susceptible to these scams due to the emotional bond that David created between them during the first two months. However, before she met him, she was divorced and was seeking a stable, sincere relationship with a partner. This was the perfect opportunity for David to quickly confess his love for her and promise a shared future. It was to make the relationship feel deep and genuine. How David was able to exploit her circumstances and desires for financial security was by presenting himself as a wealthy businessman and estate agent investor. To make this believable, he used a social media profile that featured luxury properties and business conferences. He also told Jennifer that he owned several e-commerce sites that sell

tech. In addition, he guaranteed a 50/50 profit split for the investment. This further drives the promise made about the shared future and builds up David's credibility to gain Jennifer's trust.

During each month/phase of the fraud, David created a sense of urgency and dependence to hook Jennifer in. In the third month, the housing opportunity was to trap her in, causing her to desperately protect this "once-in-a-lifetime" investment. To push the desperation to panic, David had warned her that if they didn't pay the additional $15,000 for the unexpected structural renovation cost, they would lose the house and the contractor would place a lien. In the fifth, he further validates the relationship by offering her a business partnership in his "retail business". To Jennifer, this was an exciting moment for her. Lastly, in the sixth month, when she started to get suspicious of the housing delay, David had to quickly shift Jennifer's attention back to him by putting guilt on her from an emotional hook about his personal emergency. All these tactics were able to keep Jennifer close to him.

According to the FTC (2022), the typical romance scam involves the attacker creating a fake profile on a dating site or app or contacting you through social media. The goal of this is to make the victim fall in love and trick them into giving money. These usually include small requests in gifts, emergencies, or the cost of their trips to meet with them (Graham & Smith, 2024, p.87). These scams often result in emotional and minimal financial loss. In investment scams, this involves the attacker luring the victims with promises of low or no-risk investments that turn out to be non-existent (Internet Crime Complaint Center, n.d). The goal is to get the victim to transfer money into a fake business platform. However, the attacker must establish trust before execution. These scams often result in financial losses. In this case, David managed to use both to build up trust and gain money. How he was able to do so was by first presenting himself as wealthy and building an emotional bond, then quickly hooking her in with the two investment opportunities. To back himself up, he used fake business plans, documents, and a website to look legitimate. This resulted in Jennifer being robbed of love, trust, and savings.

Part 2: Prevention Strategy

1. The five steps of verification for online investments presented through personal relationships are verifying the identity, researching the investment programs, verifying the documents, researching the registration status of the company, and meeting up in person. According to Schubert (2025), searching for the person's name, photos, and other details online would verify if the person is real. In these scams, scammers would steal photos from other people on the internet. This checks for authenticity. The next step is researching the investment programs. Using words like "scam", "review", and "fraud" while searching the company's name online, and using the individual's experience, can alert you to the problems (FTC, 2023). According to FINRA (2024), by going to the sources that have collected regulatory information, you can compare the documentation that you receive and check for inconsistencies, such as a different firm name or location. They also suggest searching up the contact information to see if

it matches the documents given by the scammer. According to the FTC (2023), you can check the background of the investor, such as the registration and license status. This is to check if the company is known to others and its reputation. Lastly, if possible, asking to meet in person would determine if they would come. This would determine if the relationship is actually genuine and reveal that the investment is fake.

The resources and tools that can be used to verify these scams are Google reverse image search, FINRA BrokerCheck, Secretary of State Business Search, and CertifID. Using Google reverse image search can allow you to upload a photo into the search bar, and it will pull images from the source. Utilizing this tool in this case would reveal the true online identity of the person. To verify the investment firms and companies, FINRA Broker Check is a tool that can help you research the professional backgrounds of brokers and investment firms (FINRA, n.d). To verify business legitimacy, the Secretary of State Business Search is able to provide detailed information about the business and its registration. This resource can be used to search for businesses in Florida. Lastly, CertifID can be used to verify real estate transactions. CertifID is a platform that verifies the identity of transaction parties and bank account details before funds are transferred. How someone can verify property ownership, business registrations, and contractor licenses is by using resources such as County Recorder Offices, SEC EDGAR, and state licensing board websites. County Recorder Offices provide information such as public records, mortgages, and deeds. Through this resource, they would be able to find information on properties within their county. SEC EDGAR is another resource that provides free access to business filings such as financial information, registrations, and reports. Lastly, using state licensing board websites allows you to navigate through state portals to find agencies and list all services. From both of these resources, they can see if registrations and licenses are active and real.

A few warning signs that should be considered when mixing romance and investment scams are the pace, interaction, and payment methods. In both romance and investment scams, the pace is usually aggressive and rushed. In romance scams, this is done by lovebombing the victim. According to Schubert (2025), scammers are often quick to say “I love you” to the individual to get their trust and personal information. In investment scams, scammers often create a sense of urgency with one-time investments for the victim to quickly give in to the decision. In addition, they can also adjust their pitch to appeal to the victim’s emotions (FINRA, 2025). As for interactions, the scammer would say they would love to meet, but cancel plans due to emergencies that prevent them from meeting (Schubert, 2025). According to the FTC (2023), scammers will tell you how to pay, whether it would be through a wire transfer, gift cards, money transfer apps, or cryptocurrency. These are payment methods that, once sent, make it difficult to get money back.

2. What Jennifer could've done at each stage of the red flags was to slow down the pace, consider meeting David, research, stop payments, and block him. In scams like these, scammers often rush to messaging apps when they meet the victim on the dating app to avoid certain controls. According to Schubert(2025), it is best to slow down and speak with a trusted person. This creates a boundary between the victim and the scammer. Not only would this provide a boundary, but also talking to a trusted person, such as a relative, can give warnings before the relationship goes any further. If she can't meet David in person, she can insist on video chats; however, she can ask David to show his face if he hasn't. This would possibly give her a clear indication of whether his face matches the profile. Through the documents given in the investment pitch and business partnership opportunity, Jennifer could use the tools mentioned in the previous paragraphs to verify if these documents are reliable or not. Once she finds out that these documents are fake, she can stop all payments and report the scam. The banks that she's associated with can recover the funds. Lastly, after the emotional guilt trip regarding David's daughter, she can immediately break all contact with him by blocking him. Usually, in emergencies, the partner would contact their family members first and not someone they just met for a full cost. Three agencies she can report these scams to are local law enforcement, the FBI's IC3, and state customer protection agencies.

The steps Jennifer can take to prevent further scams and losses are to get in contact with her banks, specifically her credit card bureaus, seek emotional support, gather information, and stay informed. Getting in contact with credit card bureaus can inform the lenders of what happened in the fraudulent transactions. This will determine whether they need to freeze or close the account (TransUnion, 2024). She can also place fraud alerts to monitor her credit and also for credit card agencies to monitor for scammer accounts that were created (Team Kentucky, n.d.). According to Team Kentucky (n.d.), credit card companies may also reverse the payments and alert other customers. Seeking emotional support, such as counseling services, can help in processing complex feelings and figuring out strategies to heal and move forward (FightCybercrime.org, 2025). Also, reaching out to family and friends can provide another perspective and emotional support. According to Team Kentucky (n.d.), they suggest not deleting anything related to the scam and saving screenshots of messages, emails, and voice messages. Jennifer can present this information to the courts as evidence. Lastly, staying informed on the latest cyber threats can keep you updated on current scams (FDIC, 2021). All of these resources and methods can help Jennifer stay protected from future scams.

The roles and responsibilities of banks, credit card companies, and payment platforms in fraud cases include investigating fraudulent activities and implementing security technologies to prevent future scams. In banks, they use security technologies like fraud detection systems. According to Leppard Law (n.d.), these systems are able to analyze transactions in real time using machine learning and artificial intelligence. Banks also collaborate with federal authorities to enhance their fraud detection (Leppard Law, n.d.). By sharing information and resources, they

can stop fraud schemes. In credit card companies, they will automatically cancel your card and send a new one, and start an investigation (DeNicola, 2020). The investigation usually takes 60 to 90 days due to gathering information about the transactions. Credit card merchants also issue measures to prevent fraud, such as virtual card numbers. This allows you to create a virtual card number to use for online transactions, while keeping your actual card number a secret (DeNicola, 2020). As for mobile payment platforms, they enable you to use two-factor authentication and PINs to secure your transactions. This makes it difficult for scammers to gain access to your accounts. They also provide customer support services for you to call when there is a problem.

Part 3: Real-World Applications

Although I'm very safe when it comes to certain things online, however, I can still be vulnerable to phishing scams and online shopping platforms. Nowadays, these phishing scams are very hard to spot due to their legitimate language and professional-looking interfaces. However, sometimes they can be obvious even if the rest of the messages look professional. For example, at ODU, there have been numerous phishing emails regarding job positions. Within the email, it includes the job position information and a form for you to put your credentials in to "apply for the position". With online shopping platforms, the products look good, but some things look sketchy, such as the payment method interface and the webpage. Three ways that I can protect myself from these potential frauds are to look for inconsistencies, verify website authenticity, and install anti-phishing software. In both phishing scams and online shopping platforms, inconsistencies involving the message or webpage may include some grammatical errors, the links not matching the domain, and may ask for information other than your credit card number. I can also look at the design of the emails to see if there are misspelled words. Verifying the website's authenticity can also reveal if the link is legitimate or not. For online shopping platforms, I can look at the URL and check for HTTPS to see if it's a secure website. Lastly, installing anti-phishing software can help detect possible phishing emails and block unsolicited contacts.

References

DeNicola, L. (2020, August 19). *How Do Credit Card Companies Investigate Fraud?* Experian. https://www.experian.com/blogs/ask-experian/how-do-credit-card-companies-investigate-fraud/

FDIC. (2021, October). *Avoiding Scams and Scammers* . FDIC. https://www.fdic.gov/consumer-resource-center/2021-10/avoiding-scams-and-scammers

Federal Trade Commission. (2022, August). *What to Know About Romance Scams*. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/what-know-about-romance-scams

Federal Trade Commission. (2023a, July). *How To Avoid a Scam*. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/how-avoid-scam

Federal Trade Commission. (2023b, December). *Investment Scams*. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/investment-scams

FightCybercrime.org. (2025, April 21). *How to Provide Support to a Loved One Involved in a Romance Scam*. FightCybercrime.org. https://fightcybercrime.org/blog/how-to-provide-support-to-a-loved-one-involved-in-a-romance-scam/

FINRA. (n.d.). *About BrokerCheck* . FINRA. Retrieved November 2, 2025, from https://www.finra.org/investors/investing/working-with-investment-professional/about-brokercheck

FINRA. (2024, March 11). *Be Alert to Signs of Imposter Investment Scams* . FINRA. https://www.finra.org/investors/insights/be-alert-signs-imposter-investment-scams

FINRA. (2025, May 28). *Relationship Investment Scams: What They Are and Tips to Avoid Them*. FINRA. https://www.finra.org/investors/insights/avoiding-relationship-investment-scams

Graham, R. S., & Smith, S. K. (2024). *Cybercrime and digital deviance*. https://doi.org/10.4324/9781003283256

Internet Crime Complaint Center (IC3). (n.d.). *Investment Fraud*. Internet Crime Complaint Center (IC3). Retrieved November 2, 2025, from https://www.ic3.gov/CrimeInfo/Investment

Leppard Law. (n.d.). *Leppard Law*. Leppard Law - Top Rated Orlando DUI Lawyers & Criminal Attorneys in Orlando; Leppard Law - Top Rated Orlando DUI Lawyers & Criminal Attorneys in Orlando. Retrieved November 2, 2025, from https://leppardlaw.com/federal/white-collar/the-role-of-banks-in-reporting-and-preventing-credit-card-fraud/

Schubert, C. (2025, February 14). *How to Detect (and Avoid) an Online Romance Scam*. Security National Bank. https://www.snbonline.com/about/news/how-to-detect-an-online-romance-scam

Team Kentucky. (n.d.). *Recover from a scam*. Team Kentucky Stop Scams. Retrieved November 2, 2025, from https://stopscams.ky.gov/scams/browser/static-content/43

TransUnion. (2024, December 27). *How to Report Fraud on Your Credit Report*. TransUnion. https://www.transunion.com/blog/identity-protection/how-to-report-fraud-on-your-credit-report