We are all investing quite a bit of hard-earned money in deals with limited information, something akin to the fog of war. Don't want to scare anyone out of investing, but the more deals I do, the more I wanted the voice of an expert. So, I called up a friend with 15 years of experience prosecuting white collar fraud cases at the highest level of federal law enforcement. We had long discussions on the best ways to protect our investments.

Bottom Line Up Front (BLUF, it is a military thing): Cultivate a framework or way of approaching investments based on actual cases and become aware of the common tactics criminals employ. We call it a "Fraud Framework."

Case Study: United States of America vs Brian Thomas Sapp (Novus Properties, LLC)

Scam Tactics:
1. Outsized Returns – Principle + 25% within 120 days
2. Guarantee of Returns
3. Fabricated Paperwork
4. Never Actually Purchased Property (Investors could have contacted prop managers or looked at county records)

2018 IC3 Report from FBI's Crime Complaint Center: Fraud is happening on a large scale.

"Your investment is only as good as the team operating it" (David Zook)

"Only invest with operators you Know, Like and Trust" (Buck Joffrey)

Fraud Framework

1. Resist the **Fear of Missing Out (FOMO).** Scammers will put use a perceived lack of time to get you to skimp on due diligence. This is a balancing act, however. Many deals need to close in 60-90 days from the time a property is put under contract. Capital raisers will need to secure funding in a short time frame and deals do fill up. Get to know the group prior to a deal happening so you trust them and are aligned with their philosophy. Are they in the market and asset type you want to target? Do they have a long history of integrity? Do you sense they are relational or transactional in their interactions?

2. Never allow **"Personal Guarantees"** to replace logical due diligence. No one can guarantee an investment. Risk exists. If the operator uses this type of language, run. We believe Multi-Family real estate done right offers an extremely attractive risk/reward profile but don't guarantee anything. You align with asset type, market, operators and accept the risks or don't do it.

3. Beware of **"Affinity Fraud."** This is investment fraud in which fraudsters preys upon members of identifiable groups, such as religious or ethnic communities, language minorities, the elderly, or professional groups.

4. Do not send money **Overseas**. You can find investments off-shore but why assume the risk when there are plenty of solid markets in the US. People from China are doing their best to place capital in real estate here. Why do you think this is the case?

5. **See, Feel and Touch the Asset**. County records should show the entity you invested in actually took ownership of the asset you purchased. Trust but verify. Visit the property, talk with the management company. Any hint in a lack of transparency is a huge red flag.

6. **Don't throw good money after bad**. If the investment isn't working out as expected, get comfortable with the explanation, communication style, etc. and be careful about upping subsequent investments.

7. Call **law enforcement** if things look fishy. Frauds don't get better with time. Trust your gut.

The Information (criminal plea) and Statement of Facts relate to a recent matter adjudicated in federal court in northern Virginia. The individual, named Brian Sapp, was convicted of executing a complex Ponzi scheme by representing to investors that he was engaged in the acquisition and rehabbing of residential properties. It is excellent food for thought for real estate investors to chew on.

The 2018 IC3 Report summarizes fraud-related crime trends observed by the FBI's Internet Crime Complaint Center.

We can chat about major trends, and I will endeavor to provide you common pitfalls that ensnare sophisticated investors. My top two themes are 1) With very few exceptions, never send your investment dollars to overseas or offshore accounts; and 2) Due diligence in all its many permutations is routinely not completed effectively by investors who become victims. Why? Greed and Fear of Missing Out (FOMO) causes investors to rush into things that seem like fantastic but fleeting opportunities. Obviously just my two cents, but I'd like to give you some material points to think about regarding side-stepping fraud.

The FBI's 2018 fraud report describes in some detail many different types of frauds that target the investing public. From stock trading manipulation to romance scams, the frauds are as varied as the victims they target. While I encourage any sophisticated investor to be reasonably familiar with the schemes and approach strategies that fraudsters implement, there are some simple and straightforward strategies to make yourself a hard target and not succumb to fraud. To really understand what makes us victims, we have to be honest with ourselves about how we approach prospective investment opportunities. By understanding why so many people rush into being defrauded, we can better protect ourselves. So, without further ado, what follows is a brief and partial list of ways to make yourself a hard target:

1. Resist the Fear of Missing Out (FOMO). Just as any experienced salesman knows how to use the hard sell to make an opportunity seem fleeting, scammers almost always employ the same strategy. By putting a short window on an investment opportunity, the scammer can force the investor to act fast. Perhaps the real estate investment only needs so many dollars and is quickly filling up. Perhaps the stock a salesmen is pitching is about to explode to the upside. While real opportunities do have shelf-lives, the fear of missing out causes investors to skip performing critical due diligence. Be careful to guard yourself against allowing your decisions to skip logical steps due to perceived lack of time.
2. Never allow personal guarantees to replace logical due diligence. An entire category of fraud is known as "affinity fraud", which has been defined as a form of investment fraud in which the fraudster preys upon members of identifiable groups, such as religious or ethnic communities, language minorities, the elderly, or professional groups. Many professional scammers behave sociopathically. Sociopaths are often extremely talented at ingratiating themselves with their potential victims. Too often, investors find themselves in a friendship with the person offering the investment, and allow the personal representations of that friend to replace logical due diligence. Be careful and

honest with yourself - are you investing money on the word of the person receiving that money? Don't ever allow personal relationships to replace commonsense verification.

3. Think hard before sending money overseas. Let's say you fall for something and agree to invest. If you send that money to a domestic bank account, there will likely be a paper-trail should investigators want to follow the money. If you discover right away that you've been defrauded, there is even a mechanism for federal law enforcement to stop and reverse your wire (see pages 11-13 in the attached IC3 Report regarding the Recovery Asset Team for more information). However, law enforcement's ability to investigate and seize fraud proceeds is drastically reduced when those funds go to overseas accounts. Sure, there are countless examples of successful investments featuring payments to overseas or offshore, but it is statistically riskier and many sophisticated fraud rings are headquartered in overseas jurisdictions. Try to keep your funds domestic, and think about keeping your investments domestic as well. Where your investment is located, after all, can drastically affect your ability to verify its existence.
4. See, feel and touch the asset. This goes to basic due diligence. Many sophisticated investors prefer real estate investments precisely because they are real, tangible assets. So take steps to ensure the asset is real. In the attached example of a real estate Ponzi scheme, Brian Sapp told investors he was purchasing specific properties with investor money. If investors had visited the county auditor website and looked up any of the properties, however, they would have readily seen that Sapp did not purchase those properties. Ensure the entity you are investing with takes title of the property you believe you are investing in. Visit that property and feel comfortable that it is what they say it is and that the photos provided to you accurately reflect reality. Interview the management company contracted to manage the asset. Believe it or not, even sophisticated fraud schemes rarely have more than one or two layers of back-stopping, and doing simple due diligence will often reveal red flags.
5. Never throw good money after bad. The mentality of victims can sometimes be puzzling to behold. Once a scammer succeeds in getting money from an investor, one would think that it would become increasingly difficult to "get" them again. However, it would seem the opposite is true. Once someone is on the hook, so to speak, they are committed to the belief that they have not been defrauded. Scammers routinely exploit this vulnerability by securing small investments up front and going back for always-greater sums. If an investment is not performing as represented, put the brakes on any subsequent investment until your concerns are addressed and your red flags resolved.
6. Do not fall for investment managers telling you that going to law enforcement will doom your investment. Guess what? If someone you invested with tells you that going to law enforcement will result in the failure of your investment, you likely did not have an investment to begin with. Legitimate investment managers simply do not say this. Again, seems logical, but many investors are lulled into inaction by just such a misrepresentation. Getting capable federal law enforcement to look at your investment and investment manager can reveal red flags that you the investor would never see.

Trust your gut - if you see/feel problems, try to find a trusted contact in law enforcement to discuss your issue. Frauds do not become better with time.

https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219