Conference Title: NFAS001 | Recent Fraud Trends and Tips for Avoiding Them

Date: October 5, 2023

Joel Giamalva: Hello, everyone, and welcome to today's webinar hosted by NFA and the CFTC. It's just past the top of the hour, so I think we're going to get things started.

My name is Joel Giamalva, and I'm a Communications Specialist at NFA, the self-regulatory organization for the US derivatives industry. I'm joined by Dan Rutherford, the Associate Director of the Office of Customer Education and Outreach at the CFTC, and JonMarc Buffa, Assistant Chief of Office of Cooperative Enforcement at the CFTC.

Before we dive into the main content of today's presentation, I know Dan has some housekeeping he'd like to address, so I'll hand it over to him.

Dan Rutherford: Thanks, Joel. Just a quick disclaimer. This presentation is provided for general, informational and educational purposes only and does not reflect or provide legal or investment advice, guidance, or interpretation to any individual or entity. The views presented herein are my - are the speaker's own and do not necessarily reflect the views of the Commodity Futures Trading Commission or the Commissioners. References to any products, services or resources, or the use of any entity, organization, trade firm or corporation name do not constitute or imply endorsement, recommendation or favoring by the CFTC or the United States government.

The CFTC does not guarantee the accuracy or completeness of any information contained in third party resources or websites referenced herein. Joel?

Joel Giamalva: Thanks, Dan. As you know, this week is World Investor Week. World Investor Week is a week-long global campaign promoted by IOSCO to raise awareness about the importance of investor education and protection and highlight the various initiatives of regulators in these two critical areas.

Ultimately, the week is designed to educate you, the investing public, on how to safely participate in the markets. Both NFA and the CFTC are members of IOSCO, and both of our organizations make investor education and protection a top priority.

This is an opportunity for Dan, JonMarc and I to provide everyone with some crucial information for investors about recent fraud trends.

Throughout the presentation, Dan, JonMarc and I will be covering a variety of topics to help you understand some of the recent fraud trends we've been seeing. JonMarc will explain the CFTC enforcement program, and then Dan will describe different fraud trends and give tips for avoiding them. I'll explain the importance of due diligence, the risks associated with impostor scams, and describe how investors can protect themselves from fraud.

Following our prepared remarks, we've allocated some time to answer any questions you might have. To ask a question, locate the box labeled Ask a Question on the left side of your webinar screen. Please type the question you would like to ask into the box and click the send button. Dan, JonMarc Mark and I will get to these questions at the end of today's presentation.

First, let's focus on the CFTC's enforcement program and the recent fraud trends they've been seeing. Dan, JonMarc, I'll pass it over to you.

JonMarc Buffa: Hi. Good afternoon, everyone. My name is JonMarc, and I run the CFTC's Office of Cooperative Enforcement. My office is designed to assist our federal and state partners, both civil and criminal work together to ensure that we can protect the public.

Just quickly on background, the CFTC was founded in 1974 as an independent federal agency. Our jurisdiction extends to derivatives, but it also extends to underlying physical commodities in the

cases of fraud and manipulation. Given that wide berth of responsibility, as you can see on the slide, we have certain areas of priorities where we are putting a lot of our resources.

The first is digital assets. As you may know, they are a very hot topic in the space. And since 2015, over 34% of our enforcement actions were regarding digital asset fraud or manipulation. It's an area that investors should be wary as they invest, and that they should be careful with their money and use only registered entities.

We have a whole host of fraud in the space of Ponzi schemes or affinity frauds. Affinity frauds are where men and women prey upon people who share some common interest or other affinity. So they go to the same church, the same synagogue. They happen to be interested in the same athletic team, and they use that friendship to convince individuals to invest with them, even though that person, in fact, is not actually a registered or authorized person to assist them.

And in many cases, they're are Ponzi schemes. And a Ponzi scheme simply is where someone uses new investor money to pay promised returns to old investors. Doing that allows them to continue the facade that they are running a legitimate business, when in fact they're not trading. Or if they are trading, they're actually losing money, and therefore they rely on new investors to allow them to continue.

The next is pool fund or hedge fund fraud. So hedge funds are where individuals pool the resources of multiple people to allow them to invest in commodities or derivatives. Interestingly, there are more CFTC registered hedge funds than there are SEC registered hedge funds. And so because of this, and because our markets are large and complex, many people believe when they invest through a commodity pool, they get the benefit of having an expert. But even though that person may claim expertise, it's an area where we find lots of fraud and many affinity frauds are actually commodity pools.

The next area is foreign currency fraud, which in the parlance of the industry is called forex. Forex is where you invest in a currency pair betting which currency will go up or down. This area is designed for professional traders to hedge or mitigate risks in foreign currency transactions, for example, General Motors selling cars in Europe. They have a currency risk about whether the dollar in the euro will maintain the same relationship they currently have. That's what those markets were intended for.

Unfortunately, many retail customers have been investing in this space, and many people who again, unregistered individuals are committing fraud in what seems to be a very transparent market, but where fraud, unfortunately is quite rampant.

The next area, which is probably about 20% of our enforcement panel - platter, excuse me, is precious metals products. That's where individuals are solicited to invest in gold, silver and other kinds of bullion. Many of these individuals are promising large returns that do not materialize. They are charging almost excessive rates of return.

So if you look at a metal transaction, metals markets don't move dramatically. And so if you're charging someone 30 or 40% commission off the top, it would take decades for that person just to breakeven, much less to make a profit. You've probably all seen commercials on television and some of the reputable shops, but there are also lots of disreputable shops.

And so we urge significant caution when you invest in precious metals, because you need to make sure you know what the actual market price of a metal is, and then compare that to what the individual is offering to sell you. For example, if you are buying a quarter ounce of gold, you need to know what the market trades in full ounces. So you need to multiply that number by four. And that's how much it should be worth.

So if they're charging you a full ounce price for a quarter ounce of metal, the odds are very strong that you're being defrauded.

Another area where we see an uptick in fraud is binary options. That is betting, to use a colloquialism, either red or black on a roulette wheel. Many of these binary options involve derivatives products and other securities products. Whether or not General Motors will go up or down. Again, this area has reputable people. It also has a large number of disreputable people. And so we urge caution if you're going to engage in binary options trading and that you vet your potential partner.

The next area where we're seeing a significant uptick is elder fraud. Sadly, fraudsters prey on the elderly because many of them are nearing or at retirement age, and therefore do not have the opportunity to make enough money to survive retirement. And so those folks can tend to be eager to chase return, and by doing so, tend to fall prey for investment opportunities where the rate of return is higher than the norm in the hopes that they can build their nest egg. Unfortunately, many of those are frauds.

Secondly, because these individuals are older and past their normal working age, it's very difficult for these people once they are victims of fraud, to go back and recoup what they've lost through employment. So we advise elderly folks to be very careful when they invest again, to ensure that they use registered individuals to represent them, and that they are careful to make sure that the pitch isn't too good to believe, but the odds are it is.

We also - CFTC works with lots of our federal partners in elder fraud initiatives. The Department of Justice, the Federal Trade Commission, the SEC.

And finally, romance scams. They're commonly known as pig butchering scams. And sadly, the purpose here is an individual pretends that he or she has a romantic interest in the victim. The

victim is then convinced that he or she could make a fortune and fall in love all at the same time. Individual gives their resources and funds to the romance scammer who then promptly steals those funds.

It is a stunningly sad combination where someone has their heart broken and their bank account broken. We recently just bought a new case at the end of this fiscal year, where we brought a case charging pig butchering, and it is, again, a growing area of fraud that we are seeing. In all these spaces, my office works very closely with our federal and state partners to ensure that if someone is a victim of fraud, that we can bring as much relief and justice to that person as possible.

If you have anything in this space where you think you may be a victim of fraud, please contact the CFTC. We'll talk about our program in a second, but this is an important opportunity for you to hopefully help us stop frauds that are ongoing.

Because of this variety of frauds in our space and given how complex some of these investment fraud schemes are, the CFTC has created a number of specialized enforcement task forces. These task forces are designed to ensure consistent application of the law, to identify best practices in identifying frauds, and then prosecuting those frauds, and to develop new approaches and ideas that will allow us to take our lessons learned from existing cases and through outreach, which Dan will talk about or through working with our partners, try to prevent fraud, or if we can't prevent it at the outset, to bring actions against the perpetrators of the fraud so that he or she is subject to justice.

The areas where we have existing task forces are spoofing and manipulative trading. Spoofing is a complex trading mechanism where you trick someone to think there is interest where there is not, thereby encouraging someone to make a trade that he or she might otherwise make. The example that many people use is Lucy with - and Lucy and Snoopy with the football. When they - the person

runs up, Lucy pulls the football away and the person falls on their face. That is, in a nutshell, what spoofing is.

We talked about this a lot already at this presentation, but understand we are committed to policing the limited extent of our jurisdiction for digital asset fraud and using all of our tools to prevent digital asset fraud. As I said before, they make up currently 34% of our enforcement platter.

Insider trading and protection of confidential information. We have an entire team dedicated to ensuring that if people are doing illegal insider trading or misusing confidential information, that those people are brought to justice. We work with closely with the Bank Secrecy Act. So if banks identify misconduct in our markets that we are alerted to that misconduct and can take steps to remedy it.

Swaps is a complicated financial product designed for professional traders to hedge or mitigate risks in their markets. Swaps, unfortunately, because there are lots of players in that space, there are some unscrupulous transactions and unscrupulous traders, and the Commission is working hard to prevent that because we have an obligation to ensure market integrity. And by ensuring the swaps market operates properly, we can ensure that the underlying products that are priced off our swaps things like your mortgage interest rate, your car loan, interest rate those products are tied to professional traders, trading swaps. And so the Commission is committed to ensuring those markets are properly policed and that the trading remains fair and transparent.

Corruption is what you thought it might be. It's where individuals are using our markets in the furtherance of corruption against a public official for a public act. We talk of romance scams a few minutes ago. We have an entire team dedicated to that.

Obviously, cybersecurity is a big issue in our markets and across the entire planet. We know that taking steps to ensure that people's information is secure, that our markets aren't hacked or

hackable, and addressing emerging technologies, things like the blockchain and other areas where the Commission and its registrants are engaged in those transactions.

And finally, environmental fraud. There are lots of carbon trading. Our chairman has conducted two carbon convenings where the commission is trying to get its arms around the voluntary carbon trading markets.

And we, of course, are interested in ESG. And so the Commission is working very hard in all of these specialized areas to ensure that our resources are used the most efficiently and that we can protect consumers from fraud, manipulation and ensure that the orderly and fair operation of our markets.

Finally, and one thing I'd like to pitch to all of you, which I hope you know about, but if you don't, I would like you to focus your attention on this. Under the Dodd-Frank Act, Congress gave the CFTC the power to pay whistleblowers for tips relating to misconduct in our markets.

If an individual comes forward and brings us credible, original information that leads to a successful enforcement action where there are sanctions imposed of over $1 million, the Commission is authorized to pay that whistleblower between 10% and 30% of the amount we recover. This is a great opportunity for those of you who have been victims of fraud or perceived fraud, have been solicited for investments that you think are too good to be true.

If you see those, please report them to the CFTC through our website at whistleblower.gov. And as I said before, if your information is original and credible and leads to a successful enforcement action of over $1 million, you could receive between 10% and 30% of what we recover.

Importantly, we have a separate fund where this money comes out of. So for all of you, please don't worry that it's going to take money away from victim restitution. It will not. This money comes from

a separate congressionally mandated fund, so the victims will get paid back while we recover. And then separately, the whistleblower will be paid. Notably, you don't need to be an insider to be a whistleblower. So if you observe misconduct, please report it even if you have no inside information. We are grateful for that.

And as you can see in the second sub-bullet, we've paid over $350 million in awards to whistleblowers. And those sanctions were based on over $3 billion worth of enforcement actions. And if you are an insider, and even if you're not, if you are a whistleblower, we provide you with privacy, confidentiality and anti-retaliation protection to ensure you remain anonymous and that your employer or whomever you raise concerns about cannot retaliate against you in an employment setting.

I highly recommend you go to whistleblower.gov. on that website, in addition to information about how the program works, we have posted a number of very, very meaningful alerts for investors where we believe there's fraud in those spaces. And if you're interested in going to that website, you can see sort of the who, what, when, where, whys of fraud that we are seeing and hopefully protect yourself.

And finally, we strongly encourage you before you invest to check out the person you're going to invest with. And Dan will talk about this more in his presentation. But the CFTC website has an opportunity on our page. You can go to it and it shows you how to check brokers through the NFA, which Joel just mentioned.

The SEC has broker check through FINRA. There are opportunities at the - if you're investing in digital assets, the state of California's Department of Financial Protection and Innovation has a website which lists all their complaints they've received about potentially unscrupulous digital asset people. So again, we recommend that you look before you invest.

And with that I'll turn it over to Dan.

Dan Rutherford: Thanks, JonMarc. So hi, I'm Dan Rutherford. I'm - lost my slide there. Sorry. I'm Dan Rutherford, Associate Director for the Office of Customer Education and Outreach. We are also a post Dodd-Frank office, and we're created by the same fund that created or that funds the whistleblower program.

Our mission is a little different, though. Our mission is to use the funding we get from the customer protection fund to develop educational initiatives to help market customers protect themselves against fraud or other violations of the Commodity Exchange Act.

And I guess the big question that everyone has is what's really driving all this fraud that, you know, JonMarc was talking about. And it really comes down to a confluence of three things: social media, low financial literacy, and to a large degree, crypto assets.

And, you know, since, you know, the pandemic, the last couple of years, the last two or three years, we've seen a lot more retail traders coming into our markets. And that's not different from what we're seeing in, you know, other markets. The securities markets are seeing the same thing.

And so we have a large number of new people coming into the markets, which means some of them are younger and that have lower - and they have lower financial literacy. They also have less experience because they haven't been in the market as long.

And surveys have shown that these younger, newer investors tend to be more reliant on social media and the influence of friends and family when it comes to getting their investing or trading information.

And so those are, you know, kind of troubling if you think about the quality of the information that they might be getting. Most of the complaints that we receive that come in, you know, to the enforcement division involve the cash market, crypto asset trading area. So a lot of people, who have either been taken advantage through these romance scams or through fake platforms, what have you. Most of the complaints that we see involve crypto. And most of those frauds originate on social media.

So just to give you some idea. We had a presentation yesterday, and we're speaking with folks from the FTC. And one of the things that they've mentioned was, you know, if we look back at 2019, the losses to fraud through social media back in 2019 was about $113 million for that year. By 2022, it had grown to over $1.2 billion. So that's quite a big increase over, you know, just three years. And 2023, at least through June, seems to be on track to exceed that 2022 number.

In the first six months of 2023, more than 50% of the money that was reported lost to fraud to the FTC was through - was because of social media. And those all went to investment or trading scams.

So social media is a pretty big issue when it comes to trading and investment fraud, and the reason why that is, is because the platforms themselves, the way social media works enables fraud to occur. So typically when we talk about fraud or when people experience fraud, it goes through four basic steps. The first is, you know, people out there looking for information. They might be shopping around, they might be looking for new opportunities, what have you.

And while they're out there asking questions, that opens them up, that exposes them to potential fraudsters who might be out there. You might think about it. You know, the more you leave the house, the more likely you are to run into crime, right? Same thing here. The more you're out there in the marketplace, the more likely you are to run into someone who's trying to do you ill will.

The next step is targeting, and that's when you catch the attention of a fraudster. And maybe they, you know, are pulling your information off social media and sizing you up as a potential target. Or maybe they're sending a message to a group chat, or maybe they're advertising to a specific set of customers on the platform, and you just happen to be among them.

The next step is engagement, and that's when that conversation occurs between the fraudster and the individual who's being targeted, right?

And the last step, of course, is victimization when someone loses money. Now, the good news is not everybody who exposes themselves out there to fraud is targeted. And not all targets engage, and not all people who engage are victimized. So there's some good news there. And that I think a big part of my job is making sure that we break that chain somewhere along that way, along that path.

So again, if we think about how social media works, the algorithms themselves kind of work against you. There's an algorithm known as the People you May Know algorithm and you might be familiar with this when you're given friend suggestions, for example. The way that works is you might think of it as closing triangles, okay?

So if I am friends with JonMarc and JonMarc is friends with Joel, then I'm going to get a recommendation for Joel to be my friend. Essentially, that's how it works. But what it does is creates groups within the network that - of people that tend to share a lot of the same beliefs and attitudes, right?

So you might think about, you know, if I'm a risk seeking speculator, I am more likely to like the things that other risk seeking speculators like. And so if I'm someone who's looking to target that group, I would choose my advertising strategy to target just that group.

Now that does two things. One, it's more effective for the fraudster essentially, but it also hides those messages from the public at large and from those in law enforcement, or from regulators who are trying to keep a handle on fraud.

The next sort of algorithm is the sense and suggest algorithm. And this is what determines what you see when you log in to YouTube, when you turn on TikTok, when you go to Facebook and you see your newsfeed. Those are all sense and suggest algorithms. So they're developed to think about what you've looked at in the past and bring up similar information for to catch your attention and keep you engaged on the platform.

Again, if I'm someone who has a habit or who even has been out there researching, say how to trade forex, for example, the next thing I know I'm going to start seeing every advertisement and every other video about trading forex. So if you're susceptible to fraud or, you know, might be a little overconfident in your abilities, that could lead you into a bad situation.

Next is difficult to report fraud on a lot of the social media platforms, but it's still worthwhile. If you see something out there that looks suspicious, report it, block the individual. Now, blocking doesn't get rid of the fraud, but it signals the platform that there's something there that's problematic. And so enough people start doing that, then it's more likely to raise the signal that this is, you know, bad information and something that should be removed.

And again, I've already mentioned the targeting aspects of it.

Another trick that the fraudsters will use is called cross platforming. And imagine that you're on Facebook and you're approached by someone who wants to start a conversation about the latest, greatest token and the opportunities that abound on this new trading platform or what have you.

Well, the first thing they're going to try to do is say, why don't you come join my discord or join my WhatsApp or, you know, join my telegram group. And the reason why they're doing that is to take you off the primary platform and into a place where they can kind of control the environment and control the situation.

And the reason why they do that is because, you know, the bigger platforms, they have AI that also looks for fraud. So if you're moving from the main stage to a secluded room or side alley somewhere, it's harder. They can't detect that anymore. So if you're ever instructed to, you know, join a telegram group or join a discord group, be very, very cautious because you could be, again, going off the main stage and into that side room where, again, a lot of fraud occurs.

There's a lot of low quality information and disinformation out there from influencers. Now, the social aspect of social media is to make friends and listen to what other people have to say. But the thing that we have to remember is that they might be fairly new to the game as well. And so taking advice from someone you're not that familiar with may not necessarily be the greatest source of information for you.

And when we're talking about platforms, social media, they're built around a business model to keep you engaged and to keep you on the platform. And so a lot of questions have been raised about, you know, are they taking all the necessary steps they can to stop fraud, to stop bad influencers, to stop a lot of these things that are going on. And the answer is we just don't know, because they tend not to, you know, provide a lot of data about what's going on under the hood. And so a lot of that's TBD.

The bottom line is you need to be careful. You need to be responsible when you're out there on social media.

In terms of financial literacy, really what we're talking about is risk literacy. And these are risk markets. You know, financial literacy is low across the board, and we've known that for a long time. In fact, dating back to 2009, there's been a set number of survey questions about five questions that keep - that researchers use year-after-year to sort of measure whether or not financial literacy is going up or going down or staying sideways or what have you.

Those five questions include one question around risk. And when you look back over time, the lowest area among all of those questions are the risk questions. So financial literacy is low, but risk literacy is the lowest among them in terms of the specific domains of knowledge.

Risk is the unknown. I mean, there's no real way that you can get around it. It's always going to be there when you trade or when you invest. You know, there's counterparty risk. Who are you giving your money to? You know, if you're dealing with an unregistered entity, you really don't know. There's information asymmetry. There's, you know, a new trader is not going to know as much as a more experienced trader. Or, you know, if you're dealing with securities, you know, the seller of the security may know a lot more about that company or that product than the buyer of that security. So there's always going to be that risk level there.

And of course, there's the future. No one can really predict the future. Even in today's AI enabled predictive world, no one can really tell us what's going to happen tomorrow.

And that failure to understand risk leads to a number of problems, right? Misunderstanding, risk and return is probably the biggest one. Now people typically say, you know, well, you take greater risk, you get better returns. Well, I like to flip that around and think about it the other way. If you're chasing greater returns, you're likely assuming a lot more risk. And that's the way people really should be thinking about this.

If you don't understand risk and how to manage it, a lot of people or a lot of times you could be taking on way too much, not using the right sort of risk management tools and strategies.

And of course, the last bit of this, and where it all ties back into fraud, is that willingness to believe what's too good to be true. I mean, if you go to a website and they say, you know, you can invest in this trading plan, and if you give us $500, we'll give you back 10%. And if you give us $1,000, we'll give you 50%. You know, for one thing, there's no such thing as guaranteed returns. And it doesn't really matter how much you give them. It doesn't change - you know, how much you deposit doesn't change the risk profile of what you're trading.

But if you don't know about risk, you're going to make that mistake. And a lot of people do.

So what we try to focus on, you know, before you commit any money to a trade or to an investment, you know, take the time to learn about the markets, learn about the products. You know, how do they operate? How do they make or lose money? And if you're thinking about crypto, do you understand the tech, the tokenomics behind the tokens? If you don't, then maybe you should be putting your money there. You want to know what risks are involved? What are the operational risks? What are the cybersecurity risks?

We're all familiar with market risk and volatility. But what does that look like for this particular product. And of course where are the fraud risks? What are the common frauds in that particular market.

Finally, have a plan. You know, when we're talking - what we're talking about here is risk management. Determine how much risk capital you could really afford to, you know, place on a trade. How much can you afford to lose? And think about how much risk - how that risk capital amount fits into your overall financial plan. You know, have the living expenses covered. You have all your short term savings needs covered, your longer term savings needs like retirement, college.

And if all the answers to that - you have all those bases covered, then maybe you have money left over to speculate. And that's where that risk capital should be coming from. We always say, you know, don't invest more than you can lose, but, you know, really sit down and put pen to paper and think about what that amount is. Otherwise, you'll turn out like a lot of other people out there that, you know, go all in on the next big token, hoping it'll, you know, go to the moon and when the markets go the other way and you need to pull money out because, you know, you need a car repair.

Well, you know, you just lost a big part of your savings or investment right there.

Think about your investment strategy. Are you going to be a holder? Are you going to be someone who holds on to that particular asset for a long term? Or are you going to be a speculator?

And be reflective. Think about, you know, did you cover all the bases? Did you think about all the possibilities? And do you have risk management steps in place to handle all of that? And then think about, okay, well how much time am I going to need going forward? I got to monitor my trading. And I'm probably also going to want to keep up with the news and learn about some of the new trends. So how much time is all of that going to take? And build all of that into your plan.

When we talk about fraud risk, especially when we talk about crypto, you know, most of the frauds that - again, that we see start on social media and the biggest majority of them involve bitcoin or stablecoins. The reason is pretty simple. I mean, they're easily electronically transferable so they can move around as easily as an email. And the use of public and private keys hide real world identities.

And once a transaction is made and it's put on the blockchain and it's been verified, that transaction is final, you can't get your money back. And for the fraudsters perspective it's easily convertible.

They can turn it back into cash or they can use that funding for, you know, to buy something on the dark web, like more names of more victims.

In an online environment, the bottom line is anything can be faked. The people that you meet on social media, those profiles could be hacked. They could be made up. You could get emails from brands that you're familiar with, but those brands might actually be spoofed. So they might look just like the - like your bank or your broker. But when you go to that website, maybe there is a slight difference in the address bar and the address line of the website.

Platforms. If you're going to an unregistered trading platform, you know a lot of those can be made up. And especially the data, the balances, the performance that they're showing you on that website can also all be made up.

And a lot of times when people get involved in these types of frauds, they don't know it until they go to try and take their money out and are then told they have to pay a tax or a fee or something else, and they never get their money back.

So here are some of the red flags that you want to avoid. This is actually available on our website. It's called Curious about Crypto? Watch out for the Red Flags. The URL will be in the slides.

I do want to touch on this. However, this is the signs of a fraudulent site. And especially when we're talking about crypto and forex, a lot of these operate offshore and they're unregistered. And so these are some of the warning signs that you really want to look for, you know, does it have an offshore address? Does it have a fake address? How are you going to tell, right? It's very simple. If they have a street address printed on their website, copy that street address and do a street level map search so that you can do a virtual visit of that location.

And if you're going to a vacant lot or a gas station, as opposed to a, you know, a downtown business building, you might want to be suspicious of that platform. There's no phone number or customer service line. And really, what we're talking about here are landlines, 800 numbers or 888 numbers that you're - probably most of you are familiar with.

If there's a WhatsApp number, if it's just a live chat or email or a contact us box, forget about it. Those - you know, if that website disappears with your money, any way of contacting them disappears with it.

The website page doesn't match its claim. So a lot of these fraudulent websites will say they have billions under management, or they transact hundreds of millions of trades a day and have, you know, over a million customers in six continents. But when you do a URL lookup of their domain registration, you find out that the website is only a few months old, doesn't really add up. A lot of these websites will put up awards if they say they've won, but there's real - you know, you don't recognize who gave them.

And if that's the case, those awards are probably made up and they're just kind of build credibility. And the same for on-site testimonials. Do a search for third party reviews, look up the site's domain name plus the word scam, fraud, or reviews and see what others have said about them.

And then lastly, look for broken links, bad spelling, poor grammar, etc.

And with that, I'll turn it back over to Joel.

Joel Giamalva: Great. Thanks, Dan. Thank you both for all the information. I'd like to start by addressing the importance of due diligence before making investment decisions. NFA's Basic System is a free online tool that investors can use to research the background of derivatives industry firms and

professionals. Basic contains a variety of data points on entities in our industry, including registration information, disciplinary history, and more.

In Basic, the profile for any currently approved NFA member firm, like this one, displays a green NFA member approved banner below the firm's name and NFA ID number. NFA members are overseen by NFA.

A variety of non-member firms also have NFA ID numbers and appear in basic, such as firms exempt from CFTC registration and NFA membership, former NFA members and firms who are pending NFA membership, among others. These sorts of entities are not overseen by NFA, even though they have NFA ID numbers and appear in Basic.

Their profiles contain yellow, orange, and red banners displaying language like not an NFA member, NFA member, pending or permanently barred, among others. We've recently seen scammers attempting to confuse investors by implying that any firm listed in Basic is NFA regulated, although that is not the case.

To avoid these scams, take the following approach. First, when a derivatives industry firm or professional provides you an NFA ID, search for the ID in Basic. Firms with Basic profiles displaying an orange banner titled not an NFA member as seen here are not currently NFA members.

Firms with Basic profiles displaying a pending membership banner as seen here, are not currently NFA members either. These firms should not be soliciting customers or conducting any business as they have not yet been approved.

Here are some final points to remember when using Basic to authenticate credentials. Confirm that the name, main business address, and phone number listed on the Basic profile exactly match the name, main business address, and phone number used by the firm or professional soliciting you.

Illegitimate firms sometimes utilize names similar to those of current NFA members in an effort to deceive investors. For example, ABC Commodities, LLC., Is not the same as ABC Limited. And remember, an NFA ID alone does not demonstrate NFA membership.

Reach out to NFA's Information Center using the details shown if you have any doubts about a firm's legitimacy. NFA's Information Center representatives are also available to answer any investor questions and provide additional information on any NFA related topic.

Now we'll talk about imposter frauds. Imposter fraud can take on many different forms, but put simply, imposter product consists of scammers pretending to be someone the victim trusts in order to convince them to send money or personal information.

Scammers may pretend to be someone you already know, such as a family member or friend, and they may reach out to you through calls, emails, text messages or social media messages. They may also lie about having respected credentials, such as working for a government organization or a financial regulator like NFA.

Be skeptical of all requests for money and information, especially high pressure requests mentioning an emergency or threatening negative consequences if demands aren't met.

Recently, we've seen scammers pose as NFA staff or agents to gain the trust of potential victims. In these frauds, the scammers target recently defrauded victims, promising assistance in recovering funds lost or a fee, and requesting the victims provide bank or credit card information.

NFA reminds investors that NFA staff will never solicit payment or fees from investors for any reason. Remember to never provide your bank account or credit card information in response to unsolicited requests, or to someone you do not know and investigate and verify the legitimacy of

any people, organizations and websites that contact you, particularly when unsolicited. To verify the legitimacy of any communication or request purportedly sent by an NFA employee, again, reach out to our information center.

Here are just a few more things to always keep in mind when it comes to protecting yourself. First, always ask for written materials. Legitimate firms looking to conduct legitimate business will never have a problem providing written information.

Second, beware of get rich quick schemes. If it sounds too good to be true, it probably is. Be particularly vigilant if you have recently retired or came into money and are looking for safe investments. It's also crucial that you always stay alert when you're online. Today, you can receive investment pitches and other communications through social media posts and texts. It's no longer just the cold call or flyer in the mail.

It's best to avoid these communications or to have a solid plan for refusing these offers. Especially when it comes to cold calls and other unsolicited communications, you do not have to be polite. Simply hanging up the phone, deleting a text or email, or blocking a social media account are solid steps towards protecting yourself.

As a final tip, be wary of fake websites that appear identical to official business websites or use similar names to deceive investors into sharing sensitive information and financial resources. Before submitting any information, verify the legitimacy of firm websites.

Before we turn to your questions, dan and I want to pass along information about the investor resources and materials available on our websites.

NFA has an investor specific web page that has our latest investor newsletters, information on best practices for investors who are just getting started with investing, FAQS, information on arbitration

services, and an archive of investor education materials and resources. You can also subscribe to NFA's investor mailings to stay up to date on the latest information, including warnings about fraud and news about upcoming webinars and other educational events for investors.

Finally, NFA's investor webpage links to Futures Fundamentals. Futures Fundamentals is a one-stop educational resource designed to simplify and explain the complex derivatives markets. I highly recommend reviewing this website if you are new to the world of derivatives. The videos and other resources available on Futures Fundamentals are excellent educational tools for investors.

And now I'll pass it to Dan.

Dan Rutherford: Thanks, Joel. Here are some federal government resources available to you. Right there at the top is our cftc.gov Learn and Protect section. That'll open up pages to our videos, our publications, and our articles and advisories that you can take a look at.

We've also worked with the Treasury Department to collect up all of the crypto asset educational materials from all of the various federal agencies and put them on a website called mymoney.gov. So if you go to that link, that'll take you to all of those resources.

And I've also included links to investor.gov and their crypto asset resources, as well as the FTC and IRS rules when it comes to purchasing and owning digital assets. Joel?

Joel Giamalva: Thanks, Dan. It looks at this time we do not have any questions for anyone to answer. We'll wait a few moments for you to ask any questions you might have. If not, we'll be sure to end the webinar or answer the questions after this webinar.

Okay, well, I don't see any questions. Be sure to reach out to us at the CFTC and NFA if you have any questions. But I believe that's going to do it for today's webinar. Before we sign off today, I want

to remind everybody that you will be able to access both a transcript and a recording of today's webinar on NFA's website in the coming weeks. You can reference that at any time if you want to go over what we've covered today.

I want to thank you all again for joining. I hope you've learned something new and enjoyed the webinar. Thank you all, and have a great day.