Deconstructing to Disrupt Fraud—A Live Webinar Featuring Professor Arda Akartuna
October 7, 2025

Joel Giamalva: Hello everyone, and welcome to today's webinar hosted by NFA, the CFTC and FINRA. It's just past the top of the hour. So, I think we're going to get things started here. My name is Joel Giamalva. I'm a Communications Specialist at NFA, the self-regulatory organization for the U.S. derivatives industry. I'm joined by Jorge Herrada, Acting Director of the Office of Customer Education and Outreach at the CFTC, and Gerri Walsh, Senior Vice President of Investor Education at FINRA.

Welcome to our webinar, "Deconstructing to Disrupt Fraud." This webinar is held in honor of World Investor Week, a worldwide celebration of financial literacy and investor protection sponsored by IOSCO. Ultimately, the week is designed to educate you, the investing public, on how to safely participate in the markets. During the first session of today's webinar, we'll hear from Dr. Arda Akartuna, who will discuss how criminals are using artificial intelligence to scam victims. During the second session, we'll hear from NFA, FINRA, and CFTC on how the public can protect themselves from scams.

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. We will get to these questions at the end of today's presentation. I'll now turn it over to Jorge Herrada to introduce Dr. Arda Akartuna. Jorge?

Jorge Herrada: Thanks, Joel, and thanks to NFA for hosting this important webinar. Before I begin, I need to give a disclaimer that the views I'm about to share do not necessarily reflect the views of the Commodity Futures Trading Commission staff, Chairman or the Commissioners. References to any products, services or resources, or the use of any entity, organization, trade firm or corporation name, does not constitute or imply endorsement, recommendation or favoring by the CFTC or the U.S. government.

Now that we have that out of the way, I'd like to introduce our guest speaker. This is our panel one, "The Rise of AI and Scams." So, Dr. Arda Akartuna is an Assistant Professor at CityU Hong Kong, focusing on emerging technologies and future crime. His research looks into the prevention of future crimes that involve emerging technologies, including Web3, crypto assets, decentralized finance, central bank digital currencies, AI, new payment methods and developments in fintech. He has experience in blockchain analytics, crypto crime investigations, dark web research and open source intelligence.

His research uses both academic and practitioner experience, as well as innovative methods such as horizon scanning and crime scripting to devise preventative frameworks and early detection mechanisms. He has advised numerous private, governmental, and international organizations on future crime threats and possible prevention measures. Dr. Akartuna, actually, it's a pleasure to have him. I've spoken to him in the past. He's really

one of the most knowledgeable guys in this field. So, it's fantastic to have Dr. Akartuna here with us. He's now going to show us a PowerPoint presentation. If you have any questions for Dr. Akartuna, please put them in the "Ask a question" box. As Joel mentioned, we have until 1:30 p.m. ET for this segment of the webinar. Turning it over to you, Dr. Akartuna.

Dr. Arda Akartuna: Thank you very much, Jorge, that was a great introduction. I don't need to really add anything, that was probably a better introduction than I could have made of myself. So, it's a great honor to be invited here to speak a bit about industrialized romance scams, of course, a so-called pig butchering, in the age of artificial intelligence. I will speak briefly about how these romance scammers are actually using AI, how they're exacerbating their operations, but also how AI is being used to counter those operations as well.

Now, just a brief disclaimer. You can see that the slides that you see before you have two logos on them often. One is Elliptic, a blockchain analytics company, and the other one, as Jorge said, is City University of Hong Kong. The reason for that is the research I'm about to present to you. Most of it has actually been conducted jointly by both organizations, and I will also get to some material at the end of this presentation. If you are interested in downloading any further content reports, etc., about this research that you're about to see here, conducted by both of these organizations, you are more than welcome to, and hopefully that will be useful to you.

AI and how it facilitates online romance and investment scams. Now, when we think about investment scams and romance fraud, often what comes to mind is something like this: "Oh, I'm so sorry, a wrong number." "It's okay." "Oh, it's fate that we've become acquainted. Can we be friends?" etc. This is a typical thing. I assume we imagine what a romance scam or romance investment scam looks like and how it starts off.

The thing that we need to realize, of course, and I'm sure most of us are aware, is behind the scenes of this activity sits a huge industrial-scale illicit organized crime infrastructure and operation. We have online Telegram marketplaces, for example, catering exclusively to these scammers, selling them all sorts of illicit goods and services that help them exacerbate these scams to industrial scales. You can see there, for example, a Telegram listing for fake investment sites, fake web user interfaces that they can use. Here is a message on one of these Telegram marketplaces offering up the contact details of high-net-worth individuals, which can also be used, of course, for scammers to prioritize their victims.

Here's another one. This is a listing, again on a Telegram online marketplace, selling what is presumed, what looks like is a deepfake generator software for the use of scammers to go online, do video calls with their victims while pretending to be the young man or woman that they're claiming to be. And that very much leads on to exactly how the topic of this presentation, which is AI and how AI is being exacerbated. Of course, it's very important

to note here that behind the scenes of those messages that reach the victim sits a huge illicit online ecosystem which provides illicit goods and services, including AI tools to these scammers.

Here is an example of how AI is being used by these scammers. This is actually taken from a Telegram channel, just very similar to the examples I showed you, again catering to these scammers. Now, this Telegram channel that you're seeing actually has an AI chatbot integrated into it. This message here, what you're seeing is what we assume to be a message sent by a victim to the scammer. And what the scammer is doing is they're copying and pasting this message into this Telegram chatbot giving it a prompt saying, "I want a high emotional intelligence reply." And as you can see here, what happens is that the Telegram bot responds with an AI-generated response, which we presume the scammer then copies and pastes back to the victim. We also see these kinds of Telegram channels used to bypass language barriers. Here is an example of a scammer sending an image clearly sent by a victim, a Japanese victim, and the scammer is basically saying to the chatbot, "Please give me a Japanese message response in Japanese so I can send in response to this picture." And you can see there that the chatbot does respond. We're seeing the use of AI chatbots here to bypass language barriers, bypass and essentially create more streamlined responses and high-emotion responses for scammers. Here is another example of a listing that we've seen behind the scenes on these Telegram marketplaces. This is a video, actually what it shows, and it will play it for you in a second. This is a video that shows what seems to be an AI chatbot tool on sale, which scammers can use to speak to over 50 victims at once. Now, you can imagine what that means in terms of upscaling romance scams to an industrial scale. If a scammer can sit back and relax while their chatbot is engaging with 50 victims at once, that of course massively increases the amount of people that they can potentially defraud as a result.

This is a very short video. We'll briefly play that video for you now. [Presentation].

And there you go. So that very much shows you the kind of services, illicit AI-enabled goods and services that are on sale to these scammers behind the scenes.

Another one I mentioned deepfake generator software. We're about to play for you is a bit of a video again from these Telegram channels, which show how a deepfake generator software works, especially catering to these romance scammers trying to get their victims on video calls in order to essentially very much convince them that they are indeed who they are claiming to be, i.e., young men or women or etc.

We can play this video now. We'll play a bit of it. It's a bit longer, this one, but we'll play a bit of it just so you understand the kind of services that are being offered. [Presentation].

Okay, so what you saw there is quite concerning in a sense, because you can see that it was quite convincing. Initially the scammer was pretending to be a young woman, and then they were pretending to be Elon Musk, Leonardo DiCaprio, etc. But interestingly

enough, what you will have heard of how to spot deepfakes in the past is often they would ask you to invite people to turn their faces like so, or put their hand in front of their faces, etc. And because often for earlier generation deepfake generators, that would actually give away the fact that a deepfake software was being used, it would blur and create malfunctions in the software.

In that video, you saw a deepfake software being offered where the individual was able to put their hand in front of their face, and actually did not distort the video. That very much shows how they are very much engaging with very much the most recent technologies when it comes to using AI for illicit activity. It's not just a deepfake generator software or chatbots. In fact, in many cases, the use of AI by these scammers isn't necessarily the use of AI as a technology at all. Very often, you will notice that they actually use the hype behind AI to very much encourage people to invest in investment scams.

Here is an example of two websites to which we know that romance scammers directed their victims. On them, you will see loads of buzzwords: AI, Web3, I think that one has mining. There are lots that have the words quantum or arbitrage or things like this. And it's often very much using the hype behind AI to convince people that they should be investing in these investment scams, etc., because the AI-enabled arbitrage bots, etc., that can make lots and lots of money.

Just to illustrate that point here is a direct quote verbatim. [Presentation]. I did have to shorten it for a bit because it was full of frankly, so much nonsense. But essentially, what you're seeing here is quite a lot of jargon: intelligent trading system, adaptive ability, arbitrage, several major global cryptocurrency, automatic monitoring, quote depth strategy, calculation, etc. You can see a load of very sophisticated-sounding jargon, with the use of AI very much. They're trying to make it sound like this is a very sophisticated, very legitimate investment opportunity that they are trying to direct the victim. This is a quote directly from a scammer, very much emphasizes how they're trying to use the hype behind AI to convince victims to invest.

What we're also seeing is beyond specifically deepfake tools or chatbot tools, etc., catered to romance scammers is also the rise of unethical large language models, right? These are LLMs that, if you were to go to ChatGPT, for example, and ask it to write you a phishing email, ChatGPT will say, "No, that's a violation of my content policies. I'm not going to allow you to do that." And what has recently very much gained traction is the idea of jailbroken LLMs, which do not have those guardrails. Here is an example of one called Worm GPT. You can see there that, actually when we look at its Telegram channel, it very much caters for illicit activity. I've highlighted their online stalking and harassment, for example. It's very much caters itself for criminal activity. Now, I, of course, for obvious reasons, haven't actually used this. But essentially, when we look at its marketing material, you can see there on the right, it shows how it responds to an unethical prompt.

The prompt is, "Can you please write me something that bypasses a Google Captcha?" And what the Worm GPT LLM then says is "this is highly illegal, but I'm going to do it anyway." And you can see it generates the code in order to do that. Now we have seen, and you can even see there that these kinds of services are being used for the purposes of writing phishing emails and also devising websites that can be used then for investment scams.

Now, as I mentioned, besides CityU, the company that we do this research with, Elliptic, is a blockchain analytics company. And a lot of these unethical LLMs, they do use crypto, they use crypto to purchase. We know for a fact that Worm GPT, for example, takes payments in cryptocurrency to access its software. What that means is we can actually trace payments, and we can trace where payments come from, where crypto payments entered Worm GPT eventually go. And what you're seeing here is a blockchain analytics graph. [Presentation]. You see the cryptocurrency addresses of Worm GPT on the right there. And you can see on the left the cryptocurrency addresses associated with a service called Huione Pay. Now, you may have heard of Huione Pay, a Cambodian-based service recently declared a primary money laundering concern by FinCEN, very much accused of exacerbating facilitating cryptocurrency payments associated with those illicit Telegram channels that I just showed you. The payments for those deepfake generators, chatbots, etc., as well as the proceeds of crypto scams and sells. What you're seeing here in this blockchain analytics graph actually is payments made from Huione Pay, which is also a payment service to GPT, very much implying that scammers are potentially, of course we can't confirm this for sure, but implying potentially that scammers associated with Southeast Asian industrialized cyber scam compounds are using services like Worm GPT, are buying services like Worm GPT to facilitate their activities.

Now looking a bit more at the bigger picture. Now, of course, we know for a fact that there is quite a significant problem of industrialized cyber scams in the Southeast Asia region. Of course, parts of Myanmar, Cambodia, for example, have been associated with, for example, industrial cyber scam compounds which house labor trafficking victims. And of course, what a recent UNODC report published earlier, a few months ago, in April, several months ago, in April, suggests, and also some recent reporting suggest, is that AI-enabled cyber scams, given that they appear to be quite successful in that context, have been expanding.

Last year, they found an area operating as a cyber scam compound using AI in Hong Kong, for example, where I'm based. But also recently, there have been operating similar to cyber scam compounds identified in the South Pacific and further afield in Africa, for example. So, we are noticing, based on open-source reporting and expansion, as more and more criminal organizations try to encapsulate, the illicit financial benefits that AI brings in this context.

Now, the key red flags. I did mention earlier that there are some red flags that are already outdated despite the fact that the technology in the grand scheme of things is quite recent.

But there are, of course, still things that you can look out for. Things like lip sync issues, things like the scammer refusing to turn their head during the video call. That might imply that they're using a slightly older version of deepfake generator software. Any unnatural blinking offering of unethical practices, such as, for example, if they're claiming that they've got an inside trade, for example, that you can really get in on and make loads of money. That's probably something to be aware of. If you are, for example, associated with a cryptocurrency exchange, sudden demands to withdraw loads of money by clients may imply that they might be associated with one. There might be currently, being victimized by one of these scams, etc. And again, blurring around the face as well.

As I mentioned, deep fakes generator software is becoming increasingly effective, increasingly realistic. And frankly, what I would say is there are certain red flags that have very much remained consistent with fraud over the years, which might also still be effective, even more effective than noticing the deep fakes. If you, for example, are directed by a deep fake scammer to a website that has loads of irrational promises, it gives you unrealistic year-on-year returns, for example, the use of fear-of-missing-out tactics, the use of buzzwords, claims of support from very prominent individuals. You will often see deep fakes of Elon Musk supposedly endorsing projects.

For example, if you're directed to an investment scam website that uses poor formatting, you will have noticed a few slides ago, I showed you an example of two different investment scam sites. They did not look that sophisticated at all. For those kinds of more legacy key, red flags can still be crucial in identifying this kind of activity.

Now, on the right there, you see an email that has been used as an advertising campaign by an investment scam. [Presentation]. The reason why they are sending this screenshot of this email around as an advertisement is because it basically says that, "Oh, look, your winnings, your returns from this investment have been sent back to your Bitcoin account." It's very much trying to convey to potential investors that, "Hey, look, we do return your investments. We don't just keep your money. You can withdraw your winnings." etc., very much trying to lull people into a false sense of security.

I don't know if any of you have spotted the big red flag in this email yet. [Presentation]. But actually, there are certain things that you can spot in these emails that can help you notice that it is indeed a scam. And if you haven't noticed it yet, I can show you. Essentially, what's happening here is that they're claiming that they have sent loads of Bitcoin back to the investors, Bitcoin address five CB something something something. Now, if you are aware of crypto, if you are aware of how crypto works, you would know that Bitcoin addresses can only begin with a one, a three or a BC1. That is a very telltale red flag here, that a Bitcoin address is completely made up, and that is a completely fake withdrawal.

Other things that we can do is actually use AI to detect this kind of activity. We can very much look at past blockchain transactions to identify as red flags that are associated with scams. For example, if we're seeing small amounts of money being withdrawn to the

victim's account just to lull them into a false sense of security, we can very much actually look at the ghost crypto payments, especially if there are crypto scams being used, especially if the scams are being conducted in crypto, to actually identify and automatically flag crypto wallets that are associated with these kinds of scams. So that's something that we are actually looking at using AI for to automatically detect as well.

I'd like to quickly end off with a recent bit of research that we've just recently completed at CityU, which is the use of AI to actually map the actors involved with these ecosystems. [Presentation]. So, what you're seeing here is actually a map that we've generated using AI. So essentially, what we've done here is we've basically asked Google, give us all sorts of open-source news reports themselves, for example, that UN inflection point report that I just showed you. Any material, any open-source bit of intelligence about the Myanmar cyber scam ecosystem. And we managed to identify over 1200 news reports or actual reports or policy reports, communiques, etc., that contains some insights into the businesses that are involved, the armed groups that are involved, the scam compounds that are involved, who runs them, who protects them, who profits from them, etc.

Essentially, what we were then able to do is we actually fed all of those reports into an AI using the API of Grok 4 in this case and basically asked the AI to actually identify all the relationships. Which armed group protects? Which scam compound? Who has sanctioned this individual? Who has the majority stake in this company? Which company runs this scam compound, etc.? Basically, it identifies for us all the relationships that are involved underpinning the illicit cyber scam ecosystem in Myanmar. You can see that those are the relationships in red. You can see that very much, and when we do release this research, you'll be able to zoom in, you can see that, of course, there are individuals in Australia that are involved, businesses in Australia, businesses in Indonesia, businesses in China, businesses all over the world, for example. And also armed groups in Myanmar, etc., that are involved in the cyber scam ecosystem.

You can also see the disruption that has been caused. You can see that in the blue, and also the blue signifies, for example, sanctions, arrests, crackdowns on scam compounds. China has been very effective in that. Of course, the United States very effective sanctions regime as well. And then green there, you can see is diplomatic relations, diplomatic coordination that has been done to disrupt the issue as well. So, we can actually map the entire ecosystem and the responses to this cyberscam ecosystem using AI to understand the network, the underlying infrastructure that enables this investment and romance fraud to take place.

Now, if you are interested in additional resources, I did promise you additional resources. If please do go to Elliptic.co, you'll be able to find these two reports, which actually have more details about what I've talked about today. You can see there that there is a report about our horizon scanning work into AI-enabled crime in the crypto ecosystem, but also best practices as well, which we devise by consulting experts from across different stakeholders, including regulators.

The academic articles associated with these, they're still under review, and they'll be published soon and you'll be able to therefore read a much longer form, much more analytical academic journal article on the basis of these, once they are published via the City University of Hong Kong website as well. But on that note, what I will do is I will thank you all, and I'm more than happy, of course, to take questions. Thank you very much. Over to you, Jorge.

Jorge Herrada: All right. Thank you. And thank you for that great presentation. We have two questions in the chat, so we'll go through those. Mike complimented you on your presentation, but he had a question: where do these images and videos get sourced? So, where are the sources of these images and videos that you presented today?

Dr. Arda Akartuna: It really depends on the specific images and videos that are being referred to, but essentially a lot of them will come from the Telegram groups that we've identified that are facilitating the purchase and sale of these illicit goods and services, these deepfake generators, chatbots, etc. It will very much depend on whether specific images. But most of the images I believe in this presentation are very much from the Telegram channels that are involved in the cyber scam ecosystem underpinning this industrial-scale romance and investment fraud.

Jorge Herrada: Related to that, you were also saying that some of these at their very core, they come from these different marketplaces. I'm going to mispronounce it, Huione Group and others, so, if you were a scammer in the market to purchase these things, again, maybe give us 30 seconds more about just these marketplaces that exist.

Dr. Arda Akartuna: Yeah, sure. So essentially what's going on there is in Myanmar and Cambodia, we know that there are entire compounds set up, of course, staffed by potentially hundreds of thousands of labor trafficking victims working for organized crime groups there that are actually conducting cyber-enabled romance and investment fraud at an industrial scale. And so, to facilitate that industry there is a whole secondary industry, I would say that uses Telegram, that uses these online communication tools to basically buy and sell illicit goods and services that might be useful to those scam compounds.

Now, we have seen, for example, listings for torture devices. And we know for a fact that in these cyber scam compounds, torture devices are used to punish individuals who have not met their quota, for example, or I've tried to escape, etc. So that is the ecosystem in which these kinds of goods and services are being sold.

Now, there has been recent crackdowns on these. Telegram has been quite proactive in suspending and banning certain channels that are facilitating the purchase and sale of this equipment and services. But of course, it's a game of cat and mouse as some get disrupted, new groups come up, which also continue that ecosystem. Now, again, FinCEN, for example, I think in May there was a primary money laundering concern

designation for the Huiyuan group. That's, of course, been very effective in facilitating the shutdown of some of those groups. But of course, there's also always a degree of crime, displacement. So, we're very proactive in following where the ecosystem is moving to what new services, what new infrastructure the ecosystem is moving to as a result of that disruption as well.

Jorge Herrada: Okay. One last quick question. On slide 15, you mentioned that there are certain digits that Bitcoin transactions Bitcoin addresses. Do you mind telling us one more time what the digits are, characters are for a legitimate bitcoin address?

Dr. Arda Akartuna: Yeah. So different blockchains will have different ways in which they style their addresses and transaction hashes in Bitcoin. A Bitcoin address can only begin with a one or a three, or a BC1. If there is any claim that's on Bitcoin has been sent, for example, to a bitcoin address that is 5ABC, you know that that is a fake bitcoin address. For Ethereum, for many of the blockchains like Ethereum, they will begin with OX and they will only have a, b, c, d, e, f, and any number in them. So, if, for example, you see someone claiming to have sent funds to an address, an Ethereum address, o, x a, b, f, f, j, k, q, you know for example, that is a fake address as well. So, there are all these telltale signs which you'll be able to note when you read crypto transactions, to see whether they're legitimate or not.

Jorge Herrada: All right. Well, thank you again for your very insightful presentation. Always a pleasure for me to hear you speak. I always learn something new. I'm now turn the reins back over to Joel for the second panel.

Joel Giamalva: Great. Thank you both. Yeah, we'll now get into the second part of today's webinar. I'll be asking questions to our panelists for the remainder of our time today before opening the floor to other questions. Please put any questions you have in the "Ask a Question" box whenever you think of one, and I'll make sure we cover them at the appropriate time.

In 2024, the FBI reports losses to crypto asset-related investment frauds rose to $5.8 billion. A large part of that total is due to a sophisticated online confidence scam, referred to as relationship investment scams. The scam involves a stranger developing a relationship of trust and then fleecing the victim for everything they are worth, and more. The perpetrators of this scam referred to it as a pig butchering fraud. So let's start with FINRA to learn more about these scams. Gerry, could you introduce yourself and then explain how does one get embroiled in a relationship investment scam to begin with?

Gerri Walsh: Thanks so much, Joel. I'm Gerri Walsh. I'm the SVP of Investor Education here at FINRA, the Financial Industry Regulatory Authority. And FINRA regulates one critical part of the securities industry in the United States, the member broker firms who do business in the US. And we're overseen by the Securities and Exchange Commission, but we are not ourselves part of government, and we have been monitoring relationship or romance investment scams for quite a while now. And the way that people get wrapped in, taken

into these scams. It's very human. Sometimes, as Professor Akartuna was saying, it can be a simple, misdirected text or a parent misdirected text that you respond to saying, "Hey, I'm not who you thought I was, " and then someone strikes up a conversation.

In other instances, it's some form of impostor-ing where you might be one of your social media channels and come across an advertisement for an investment club. And that brings you in, that bringing you into the investing world. Or you might be on a dating site and either someone messages you or you land on someone's profile, but the person behind that profile is a scammer. And what ends up happening is that over a period of time, trust, a relationship develops. It's not always romantic. It can sometimes be shared hobbies or shared passions, shared circumstances: we're both grandparents or something. But eventually it turns into a request for needed funds, or the opportunity to invest in some sort of can't lose investment opportunity.

Joel Giamalva: Great. Thanks, Gerri. Jorge, how did these scams work?

Jorge Herrada: Great. Thank you for that question. And Gerri alluded to it before. But first they these scammers really build that trust slowly over time. Just because you've been corresponding with someone for a while doesn't really mean you know that person. These are long cons we found with relationship investment scams. Oftentimes, it might be a total of ten injections of funds of you giving your funds to the scammers. It is a long relationship.

At some point, though, jumping back a little bit. The scammer may say they need some money or that they have some investment opportunity. Usually starts well, you know, they may say that their uncle knows a lot about cryptocurrency investment and you see that they're living this very wealthy lifestyle, and you might be enticed to try yourself. It usually starts with depositing some funds into a well-known crypto exchange, perhaps here in the U.S. But invariably, they tell you, "Hey, my uncle knows of some really great investments at this other crypto investment site. Why don't you take your funds from this well-known U.S.-based thing, turn your funds into, say, a cryptocurrency or a stablecoin, send it across to this other exchange?" And once you've transferred it, you've basically lost it. It's a legitimate-looking, but it's a fake website. They, of course, control it. And so they impersonate, basically, on the fake websites, you see yourself making huge returns, and it entices you to invest more. You see how well you're doing, and you think, "Well, I put in $2,000. Look, now I have $6,000," so you might decide to put $10,000 in. And eventually it goes back to what I was saying, that it's not unusual to make about ten deposits.

In the end, when you say, "Okay, now that I've got all these hundreds of thousands of dollars, I think I'd like to withdraw my funds." At the point at which you try to withdraw your funds, the fake investment website will say something like, "Oh, you have to pay a fee before you can withdraw it, or you have to pay taxes before you withdraw it." And every time you answer those requirements, they come up with another excuse that you will never get your funds returned.

Gerri Walsh: And that's the worst thing about these scams, is that you don't get your money back. Joel, could you tell us about some of the red flags that could indicate potential fraud that investors should be vigilant of when they're considering digital asset investment opportunities?

Joel Giamalva: Yeah. Absolutely, Gerri. When evaluating digital asset opportunities, the public should really be aware of several common warning signs that could indicate potential fraud. One red flag is the pressure to act quickly. Fraudsters often create a false sense of urgency by telling investors a digital assets opportunity is only available for a limited time, and they will miss out on huge profits if they don't act quickly. Promises of guaranteed or high returns with little or no risk should always be seen as suspicious.

Another red flag to consider, remember, if it sounds too good to be true, it probably is. It's also important to work with regulated entities, such as those registered with NFA, rather than unregistered entities. Unregistered entities are not subject to the rules, oversight, and enforcement actions of a regulator. Researching the background of the individuals and firms, offering you investments is easy and free. By using NFA's BASIC search system and FINRA's BrokerCheck, for example, investors can find the registration, license status and disciplinary history of firms and individuals.

These tools help the public avoid engaging with unregistered entities or entities with complaints or disciplinary actions filed against them. Being aware of the warning signs of fraud and taking the time to verify an individual or firm's background can help protect investors from digital asset scams.

Gerri Walsh: Joel, thank you for plugging FINRA's BrokerCheck system. I appreciate it. And NFA basic is a great tool, but could you help people understand why it's so important to work with regulated entities and individuals, such as folks who are registered with NFA and with FINRA, rather than unregistered individuals or firms?

Joel Giamalva: Sure, customers engaging in derivatives activities can really feel confident in their financial decisions when they know that the firms they choose to do business with are effectively regulated. For example, NFA's rigorous registration process ensures that firms and individuals are fit to be doing business in the derivatives industry before granting them membership.

Once an application has been received, NFA reviews the disciplinary disclosures on each application and several other sources to determine if the firm or individual has a potential statutory disqualification that may prevent registration. NFA ensures individuals seeking registration have the knowledge necessary to do business in the derivatives industry by establishing training standards and proficiency testing for persons involved in the solicitation of futures, forex and swaps transactions.

NFA also performs a robust review of a firm's operations during the application process, and these firms must provide NFA with financial statements and corresponding supporting information. Once a firm or individual becomes CFTC-registered and an NFA Member, it must operate its business in compliance with CFTC regulations as well as NFA rules. To enforce its rules when appropriate, NFA takes disciplinary actions against its Members. So really, this framework of oversight, accountability and enforcement really provides the public with an added layer of protection when working with regulated entities as opposed to unregistered individuals or firms.

So, thanks for that, Gerri. I have a question for you now. So I understand the FINRA Foundation has been researching factors that really contribute to susceptibility to financial scams. Could you explain what is the latest on that?

Gerri Walsh: I'd be happy to. Earlier this year, in June of 2025, the FINRA Foundation, alongside researchers from the Better Business Bureau, Institute for Marketplace Trust, the University of Minnesota and the Good People Research Company, released a report titled "Exposed to Scams: What Beliefs About the world are associated with Fraud victimization?" The Foundation, along with a lot of other researchers, has been looking for quite a while about all the factors that can contribute to scam susceptibility. So contextual factors like some incident that happened in your life, perhaps the loss of a job, the loss of a spouse and other types of factors like demographics, age, income, all those kinds of things. We've been really honing in on this concept of mental frames, which is really the way that you view the world.

We've seen that certain ways of thinking about the world, certain mental frames, are tied closely to scam victimization, including relationship scams. The two that were most significant were viewing opportunity as a zero-sum game where there are clear winners and clear losers. It's not the rising tide that lifts all boats. There's someone who's going to sail, and there's someone who's going to sink. But the other one is believing that the world is not a just place, that it's fundamentally unfair. Those two ways of looking at the world are associated with a greater likelihood of scam victimization. Those two ways of thinking are both all-or-nothing worldviews.

Other factors, though, as I mentioned, include the contextual factors, psychographic factors, other types of things, but we're seeing this strong correlation. And back in February of 2025, researchers, again, from the University of Minnesota and also RTI International and the Foundation surveyed a group of known victims of fraud. So these weren't people who just admitted that they were victims of fraud. In fact, several of them would not admit that they were victims of fraud. But because of prior research that the University of Minnesota had done with the US Postal Inspection Service, these were known victims of fraud.

We wanted to see whether there were social and behavioral factors, so beyond the mental frames that we're associated with scam victimization. And what we found is that engaging

in activities that increase your fraud exposure, which include things like normal routine activities. Like opening your junk mail or entering sweepstakes drawings to win prizes, answering unknown phone calls, interacting with telemarketers. All of those are tied to greater victimization. And we also saw that older age and loneliness, being financially or emotionally precarious and exhibiting risky financial preferences or behaviors, were also associated with more likely fraud victimization. And that risky financial preference, risky financial behavior was particularly strong among younger people. Those are the traits that fraudsters tend to think of as exploitable.

If I may, I'd like to turn to Jorge to ask, what should someone do if they want to verify that a new love or friend interest is somebody who they say they are?

Jorge Herrada: That's a that's a great question. And I do appreciate that, Dr. Akartuna showed us that great video in regards to face swapping. That's very impressive technology. The technology obviously is getting quite sophisticated. But as you saw in today's age of AI, anyone can pretend to be someone else. I should have used my face swapping to be Brad Pitt today, but I'm afraid you're stuck with this. But it's amazing how it can be used to do that face swapping.

One of the key things is to be suspicious of people you only meet online. There's some things that Dr. Akartuna said, but also just looking for distorted images of hands. That's something that AI has some trouble with. Strange word choices, of course. At CFTC, we recently released an advisory entitled "Criminals Increasing Use of Generative AI to Commit Fraud." So again, that's a free resource on the CFTC website.

Another thing you can do is consider reverse image searching for your new friend. Although it's not perfect because now AI is being used to generate these images. Some victims have realized they've been scammed by simply doing a reverse image search and finding out that real person they think their dating lives in a different country and is married. I don't know Gerri, if you've seen it, but I watched a three-part series on Hulu recently called "Hey, Beautiful Anatomy of a Romance Scam". Have you seen that, Gerri? I don't know if you have.

Gerri Walsh: I have not, but it's now on my list.

Jorge Herrada: Yeah, it's actually quite good. And it's a series focuses on three women from different, some in Europe and some in the US, who had lost a close to $2 million in the scam, and it could have been avoided. In this particular story, it could have been avoided if they did a reverse image search and realized a man they thought they fell in love with was not a man working on an offshore oil rig, but was actually stolen from a guy named Brian Haugen, who's actually on the show. He's an LA-based professional makeup artist. So, a reverse image search, they could have done that and found out, no, this guy is not a successful businessman somewhere else, or he's not an offshore oil working in the Gulf of Mexico in oil rig, but in fact, it's this professional makeup artist.

Am I supposed to be sorry? I don't know if I'm supposed to be asking this question or who's asking the next one.

Joel Giamalva: Go right ahead.

Jorge Herrada: Okay. Gerri, one issue many of us struggle with beyond reading a script, is how to talk with people who lost money to a financial scam without revictimizing them all over again. Gerri, the FINRA Foundation has done work in this space. What can you tell us?

Gerri Walsh: Well, we actually do have a script, and I encourage everybody to check it out when you see the resources section in the compilation for this webinar. But when you were describing the TV show, if I may still say TV show, streaming, it's really easy in hindsight to recognize a fraud. We all see it. We all see the mistake. But when you're in the moment, and especially when you're in one of the long cons that you describe, Jorge, it is really difficult to see that you are in the midst of being exploited or being defrauded. And so the most important thing when you're talking with, especially a family member or a close friend, someone that, you know, a client or a customer, for those who are in the industry, is to take a victim-centric approach and treat the person as somebody who has experienced a crime. Treat the fraud as the deception that it is.

Instead of saying, "you got tricked" you could say "scammers are criminals who use our emotions to get us to believe something that isn't true. It's not your fault." And working with AARP and the Fraud Watch Network, the Foundation actually published a resource, as I was saying, the say this, not that, that goes through some of those different kinds of things that you can say. When someone gets robbed or mugged on the street, they're a victim of a crime, but when someone has money taken from them, the headline often says that they were duped or they were conned, which makes it their fault. But it's really the criminal's fault. And that's why we want to change the way people talk about these kinds of scams, to not revictimize people all over again.

Joel Giamalva: Great. So, Jorge, back to you here. What would you tell a victim of a scam to do once they realize they've been scammed?

Jorge Herrada: Well, kind of along with what Gerri just told us, I think the really one of the most critical things is to not criticize yourself. It's so easy to think that the people that get caught up in these scams are somehow stupid, I hate using that word, but people feel horrible. Don't criticize yourself. These scams are sophisticated, they can happen to anyone.

A study that I saw recently showed that 30% of the people that fall for some of these scams have master's degrees or PhDs. The scammers have perfected their ways to get at our human emotions in a way to make us victims of these crimes. So, I like what Gerri said, this has happened to you were not responsible for this. It's the same as you would not be

if somebody carjacked you or holds you up at gunpoint. It's not your fault. They are using techniques, and they know what they're doing.

The second thing I would say is to report the scam to a financial intermediary, social media providers, to the police, to the FBI. One great website is the IC3.gov. It's a place where you can report all scams there and that goes to the FBI. The CFTC has a part of our website at CFTC.gov where you can register that you have been scammed if it's the scam involves a commodity. So that's CFTC.gov has a "Learn and Protect section," and in the "Learn and Protect," there's a section there where you can register that.

So, thank you, Joel, for that question. So, Joel, fair turn around. I've got a question for you. For new investors entering the derivatives market, why is it important to conduct due diligence, and how can it be accomplished?

Joel Giamalva: Yeah, performing due diligence is really the process of investigating and verifying information about an investment opportunity, professional or firm. Conducting research and identifying potential risks and red flags before making investment decisions, especially those involving new financial technologies, tools or products, can prevent exposure to potential frauds and scams. To perform due diligence as mentioned before, verifying the investment is offered by a registered entity is an important way to prevent potential fraud. Using NFA's Basic system, FINRA's BrokerCheck, and other tools can help the public conduct this due diligence.

Investors should also understand the risks, mechanics and fees associated with different investment products. For example, Futures Fundamentals is a one-stop educational resource designed to simplify and explain the complex derivatives markets. This collaborative effort with industry partners provides educators, students, and the investing public with articles, videos, and interactive activities intended to explain the role of the futures markets in everyday life.

Finally, investors are encouraged to ask questions. Reputable entities with transparent practices will answer your questions and give you time to consider any investment decision. If a firm or individual avoids answering your questions, pressures you to act quickly, or fails to give you satisfactory explanations, reconsider working with that entity. NFA's Information Center is available to help answer your questions or provide information about a firm or professional's NFA membership status.

Overall, due diligence empowers investors to take an active role in protecting themselves and their finances. By carefully evaluating opportunities in advance, investors are better equipped to avoid emotional or rushed decisions and recognize when offers too good to be true.

I see we are closing in on our end time here. We have five minutes left. First of all, I want to say thank you to our speakers here. And before I check on any questions you may

have, I did want to share information about some of the resources the speakers mentioned at the [inaudible] shortly here. So, take a look at those, and we'll take a look at the questions here.

I see a question here, I can ask this one to Gerri. So, this question is from Claudia. How are U.S. institutions protecting scam victims that have lost their life savings?

Gerri Walsh: That is a great question. And thank you for that, Claudia. I can speak from the perspective of the broker-dealer industry. But FINRA, several years ago, implemented some rules to deal with financial exploitation of older and vulnerable adults. And in a nutshell, what those rules do is allow a brokerage firm to put a pause on the disbursement of funds and, actually, the transaction itself, if the firm believes that there might be fraud or exploitation happening.

It also allows the firm, without violating any privacy protections, to reach out to a trusted contact that the customer has named for their account. From firms, we're hearing that some customers are reluctant to put a trusted contact on their account, but it's really a way for all of us to protect ourselves if there's a possibility of fraud happening, even if we're traveling internationally and can't be reached. It's great for the firm to be able to reach out to somebody that you trust. Not to execute anything in your account or have access to your account, just to know what's happening. So those safeguards are part of what the brokerage industry is doing to help avoid these kinds of scams.

Joel Giamalva: Great. Thank you, Gerri. I have a question here for Arda. Question here from Kevin. He asked, is there any way to put pressure on these governments to get these locations shut down? I believe these are referencing the locations that have all these scam networks there.

Dr. Arda Akartuna: Yeah, for sure. I know since the start of this year, the Chinese government has been putting a lot of pressure on the Burmese government and Cambodia as well, and also Laos as well to address some of these scam compounds. The issue is, though, that a lot of them are operating in areas which don't necessarily have strict government authority. For example, in Myanmar, we've got a civil war that's been going on since 2021, for example. So, a lot of these scam compounds has have very much appeared in areas where the authority is not necessarily present or is being dispensed by an armed group, for example, that is somewhat complicit with these crimes. So that's where the issue often lies.

But yes, of course, U.S. sanctions have helped a lot as well to raise awareness, at the very least. So, yes, international pressure, international cooperation is key, of course, to addressing these issues in that region.

Joel Giamalva: Great. Thank you, Arda. Last question here for Gerri. Can you talk more about the University of Minnesota research? Is that something that's available to educators?

Gerri Walsh: Absolutely. And I can talk all day about the foundation's research, but I won't. We have it available on the FINRA Foundation website, which is finrafoundation.org. Just click on the "Research Center," and we've got everything listed chronologically, so you'll see it right up near the top. We also, on the FINRA website, have what's called a "Member Firm Hub," and there are scam prevention resources in there that link to other research that we've done, and also to the "say this, not that" script that I mentioned.

Joel Giamalva: Great. Well, thank you, Gerri. I see we're coming to the end of our time here. So 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 presentation on NFA's website in the coming weeks. You can reference that at any time if you want to go over what was covered today. And I also encourage you to share this webinar with your colleagues so they can stay informed of the latest customer protection offerings. Thank you again, everyone, for joining. Thank you to my fellow presenters. I hope you learned something new and enjoyed the webinar. Thank you all and have a great day.