

LATONYA EADDY: Good afternoon, and welcome to today's session, Office of the Inspector General, OIG, Fraud, Waste, and Abuse.

JEREMY JEFFERSON: Good afternoon. My name is Jeremy Jefferson. I'm a Senior Special Agent with the Department of Justice, Office of the Inspector General's Fraud Detection Office. Just a little bit about me. I've been with the department for almost four years now. Prior to coming on with DOJ OIG, I was a special agent with the Department of Health and Human Services OIG, where my primary responsibility there was to investigate allegations of healthcare fraud. So, I've been investigating fraud for almost a decade now. And we're just going to walk you through some examples, tell you about some of the things that we look for, some of the cases that our office has investigated. And I want to turn it over to Rob who's going to introduce himself.

ROBERT RANSOM JR.: Hi. How's everybody doing? My name is Robert Ransom Jr. I've been with Department of Justice OIG for approximately two years. Prior to that, I was with the Drug Enforcement Administration where I investigated Title 21 violators and transitioned over to the Money Laundering and Fraud Unit, and did that for about 13 years, and transitioned here over to OIG.

JEREMY JEFFERSON: All right. Thanks, Rob. So, we'll go ahead and get started. Just a couple of housekeeping items during the presentation, if you're not already on mute, we ask that you place whatever device you're using, whether it's your phone or your computer, on mute. Any questions that you have, feel free to post them in the chat section. And at the end of our presentation, we'll circle back to you and make sure we answer all of your questions. There are some poll questions throughout the presentation and that's just to keep everyone engaged and test your knowledge. Test your fraud-fighting knowledge. So, without further ado, I'll jump right into it.

So, the Office of the Inspector General. And you'll see our mission statement here, which is to detect and deter, waste, fraud, and abuse and misconduct in Department of Justice programs and personnel, and to promote economy and efficiency in those programs. So, three words you'll hear me refer to often throughout this presentation, waste, fraud, and abuse. When you think of any OIG component, whether it's the Department of Veterans Affairs OIG, the Department of Health and Human Services OIG, every OIG is in place for those three words – to detect and deter, waste, fraud, and abuse from occurring within their specific programs. When you think about the Department of Justice OIG, I want you to take away a couple of things, but remember, a

number of you are already Department of Justice grantees, maybe you're in line to receive funding from the Department of Justice. With that, it gives us as the OIG, the authority to oversee those funds. To ensure that those funds are being used appropriately. So, that's just our agency at a very high level.

So, grants and grant fraud. I want to take a moment just to talk about grants. I'm sure you've heard this before, so I'm going to be real brief on this slide, but essentially, every grant goes through what we call a lifecycle. Or a lifecycle timeline. And that timeline's going to start with the pre-award phase. During the pre-award phase, that's essentially when the government is formally announcing an opportunity. They're formally announcing it to the public saying, "We are giving out grant funds for this specific purpose or mission." And from there, you transition into the award phase. And that's the particular phase where funds are actually dispersed, they're given out. And then you have the post-award phase, which is essentially a report card. There're various audits that can occur during this phase. It's where your performance is analyzed and it's essentially your report card. So, that's at a high level, the grant lifecycle timeline.

So, grant fraud. I've been a white-collar investigator for quite some time now and I often get asked the question, "Hey, man, what is it that you do, right? What is grant fraud? I really don't understand what grant fraud is, how it works. What is grant fraud?" I get asked that question all the time, whether it is at family cookouts or what have you. It's the question that often comes up. So, to keep it simple, what I tell people is, "Well, grant fraud is essentially lying, cheating, and stealing." Lying, cheating, and stealing, that's it. Lying, cheating, and stealing anywhere throughout this timeline, throughout this grant lifecycle constitutes grant fraud. I want to talk about risk here in a second. But when you think about grant fraud, whether it's inflating your credentials during your pre-award phase, maybe saying that you have a state-of-the-art facility where you plan to house victims of domestic violence – maybe you're inflating your credentials. Or it could be during the award phase where we've seen stealing. We've seen individuals steal funds from the government during the award phase in a variety of different ways. Or whether it's lying or cheating during the post-award phase. And that can look different in a couple of ways. That could be falsifying documentation. Or not having transactions that are within arm's length when you're sub-granting out some of these awards. So, essentially, if someone asks me what grant fraud is, I'm going to tell them, "It's simple -- it's lying, cheating, and stealing anywhere in this process." Anywhere in this process, lying, cheating, and stealing constitutes grant fraud.

Now, I want to spend some time talking about risk, because this is extremely important when you think about grant fraud and grant fraud investigations. When you're thinking about risk, every organization, regardless of size, regardless of mission, regardless of

income, revenue, every organization has some level of risk. That's just a fact. When combating risk, when analyzing, and evaluating the practices of your organization, we don't want you to operate like this individual here, whose head is in the sand. They're not aware of what's going on within their organization, within their company. We don't want you to operate like this individual here. We want you to operate like this individual here. They are on the lookout for potential grant fraud risk. I tell the grantees I give these presentations to and these briefs to, I said, "Look, I'm not going to be able to make you a fraud-fighting investigator in a 45, 30-minute presentation." I'm not going to be able to do that, right? But what I hope you take away from this presentation is that you have to be aware of risk, know that you have some risk and know that grant fraud can occur within your organization. Because the first step of mitigating risk is identifying risk. We want to make sure that, "Hey, we are aware that things – these things can happen. What internal controls can we put in place today to mitigate that risk?" So, that's what I want to do. That's my goal in this 30, 45-minute presentation. Rob and I's goal, we just want to make you aware, we want to raise awareness here, because again, we're not going to be able to make you Department of Justice Special Agents that can identify and investigate fraud. That's not our goal here. Our goal is to raise awareness.

The consequences of grant fraud can be significant, and I can't understate that. They can be significant. And they can range from your business being shut down – because there're a lot of organizations that operate solely off of grant funding. If that grant funding is removed, that organization can be shut down. There're a number of different administrative remedies that the government can use if it identifies one instance of grant fraud occurring within your organization. We'll talk here about the False Claims Act and the civil monetary penalties that can come with, or be associated with, one instance of grant fraud occurring within your organization. And last but not least, you can end up in prison. And I can't stress that enough and I want that to be taken seriously. Because we'll go through some case examples, a lot of investigations Rob or myself have had the opportunity to work on or work with partner agencies, but there has been several occasions where grant fraud has risen to the level of criminal prosecution. So, again, we're focusing on prevention here. We're focusing on prevention, but we want you to be aware that there are situations where grant fraud has risen to the level of criminal prosecution. It can happen.

So, this brings us to our first poll question. I'm going to launch it. It says, "Grant fraud can result in administrative remedies, such as a grantee being required to repay funds, civil remedies, such as the federal government suing a grantee for penalties and damages, and/or criminal remedies which could include criminal prosecution with potential jail time and restitution." So, when you all have a moment, feel free to answer

that poll, make sure that it's loud. And I am seeing a lot of trues, which is correct. There're still a couple people. And that's correct. The government can use a combination or any of these remedies if it identifies one, just one instance of grant fraud occurring within your organization. So, let's be mindful of that.

So, this slide here is mandatory disclosures. I'll read the highlighted portion. "The non-federal entity or applicant for federal award must disclose in a timely manner in writing to the federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, robbery, or gratuity violations potentially affecting the Federal award." So, essentially, what is that saying? If you become aware of an instance of grant fraud occurring within your organization or your federal award, you are required to notify the government in writing. The NDAA, National Defense Authorization Act of 2013 – this is whistleblower protection. So, if you're an employee of a grantee or sub-grantee, and you report fraud, it is illegal for you to be discharged, demoted, or otherwise discriminated.

I'm going to talk about lying, cheating, and stealing, and I want to break each one down. So, you can get an understanding of what it may look like. The majority of our investigations, the open investigations we have currently ongoing in our office, encompass either one or all three of these schemes. The first one I want to talk about is lying.

So, what is lying? A grant agreement is essentially a legally binding contract. What that is, is it's extremely important that you are familiar with key provisions, the ins and outs, all of the texts, everything in your grant agreement. It's essential that you know what's in that agreement, you have to know what's in your agreement inside and out. Grantees must act with integrity when applying for and reporting the actual use of their funds, okay. The third point – you're obligated to properly track the use of these funds and maintain supporting documentation. And we'll talk about some case examples a little bit later. But those are some points with lying. Typical issues in this area that we see in our investigations, the first point is using the funds in a manner different than outlined in your grant agreement. For example – and again, this is just from some of the experience and investigations that we've worked. That first point, using the funds in a manner different than outlined in the grant agreement. For example, if in your grant agreement you have X-amount of dollars allotted for training, those funds should be used for training and not to purchase personal vehicles and/or vacations. You have to use the funds in the manner outlined in your agreement. The second point – and I mentioned this already – you have to track these expenses. You have to track them. You have to have some system in place so if and when the OIG shows up for an audit, or we begin subpoenaing documentation or requesting supporting documentation for a

drawdown, you should be able to provide supporting documentation to support that drawdown. You've got to be able to track, right? You shouldn't be commingling or mixing funds, and I'll give you a case example here briefly where an organization was commingling funds. In the last point, grantees must accurately represent their eligibility for funding. It cannot provide false or misleading information. So, what do I mean by that? If, in your application, when you apply for grant funding, if you reported that you have – again, I'll use the example I talked about earlier – a state of the art facility, you have numerous credentialed employees on staff, you have this written agreement or this written plan to where you want to combat fraud, waste, and abuse and you have this robust system in place – if you report that in your application, if and when the government shows up for an audit, they're likely going to want to see that. So, what I'm saying is, you have to be honest about what it is you have in terms of credentials, staffing, facilities, whatever the case may be, because that can be considered as inflating your credentials.

So, let's talk about some real-life case examples. So, this particular case, here was a religious group that received grant funding for security cameras. And in the pre-award phase, they reported to have a very robust accounting system, a very robust system, and policies and procedures in place to protect grant funds. Well, it was an audit, government shows up, they want to see documentation, they want to see how these procedures were in place, and they refused. They said, "No, we're not going to show you." That's not an acceptable answer. And as a result of the False Claims Act, they were required to pay back just over \$844,000. Now, I want you to keep in mind, with the False Claims Act, this organization only received about \$250,000. But because of the False Claims Act, the government – which gives the government the authority to not only recoup what was paid out, but also impose additional fines and penalties. So, as mentioned, it can have very aggressive or very significant penalties.

Failure to fulfill a key grant provision. This goes back to what I was taking about earlier where you need to know the ins and outs of your grant. I just want to tell you a little bit about this case here. It was a grantee that ran a foster grandparent program. And in this particular program, they had volunteers that went out into the community and interacted with the elderly population. These volunteers, as a provision in their grant, were supposed to have legitimate background checks. So, every volunteer that goes out and interacts with the community, they need a background check. It was found out that in an effort to conceal what had happened, this particular grantee did not perform the required background checks. In an effort to conceal that, they cut and pasted legitimate background checks from employees that have them, and then put them in the files of the employees that didn't have them. So, a couple things I want to mention with this particular case. As an OIG Investigator, we are trained to find these types of

discrepancies. We're not the traditional agents you may see on television that are jumping out of helicopters and getting into high-speed chases, that's just not who we are. We are trained to look at paperwork, to look at documentation, and identify discrepancies. That's what we're trained to do. So, more often than not, if you attempt to conceal something in your paperwork, in your documentation, more often than not, we're going to catch it. And that's just me being completely honest. More often than not, we're going to catch it. So, in the event that you do not fulfill a key grant provision, instead of trying to cover it up, it's probably best to come clean and say, "Hey, this is what happened." Because chances are, we're going to find it. So, just wanted to make you aware of that in this particular case here, why it's important to make sure you know the ins and outs of your grant.

Commingling. So, I mentioned this a little bit earlier where Big Brothers and Big Sisters of America – I'm sure we've all heard of them – agree to pay the United States \$1.6 million to resolve allegations of false claims related to their comingling of \$10 million in grant funds with general operating funds. This is a good example of having to be able to adequately track and account for expenses used or paid for by grant funds. You've got to have a system in place to track. Now, I can't tell you what that system needs to look like, you need to work with your representative on that. Your grant representative. But you have to have a system in place to track expenditures. You have to have a system in place to ensure that, "Okay, I have this source of income from this particular outlet, and this source of income from grant funds." You have to be able to distinguish what came from where. So, that's an example of commingling and why it's important to be able to distinguish where different funds are coming from.

Which brings us to our second poll question. And I'm going to launch it here. Grantees can use award funds for: A. To cover up budget shortfalls in other government programs. B. To build up cash reserves in case of a crisis. C. To make a profit. D. For any public purpose. Or E. Only for costs that are allowable, allocable, and reasonable and are within the scope of their grant agreement. So, give you some time to answer. So, the correct answer is E. Only for costs that are allowable, allocable, and reasonable and are within the scope of their grant agreement. Great job.

Move on. So, let's talk about cheating. So, in terms of cheating, grantees are required to use federal funds in the best interest of their program. Not in the best interest of a family member, not in the best interest of a friend – the best interest of their program. These decisions must be free of undisclosed personal or organizational conflicts of interest, both in appearance and fact, okay? The issues in this area that we see, purchasing goods or services, or hiring an individual from a related party such as a family member, okay? Let me give you an example. Rob Ransom and I are co-hosting this webinar. For

the purpose of this example, let's say Rob Ransom and I are brothers. Rob is my brother; I've received grant funding from the government. My brother, Rob, has a transportation company that I would like to sub-grant with. Or sub-grant some of the award to for the transportation needs of my particular organization. The problem with Rob and him taking on that portion of my business is that his quotes are two times higher than everyone else and his service is not as good. He has bad reviews in the community. It just doesn't make sense. And he charges twice as much as any other transportation company within our area. That's a potential conflict of interest. It's not saying that you can't hire friends or family, but you should be able to articulate why you selected this vendor over another. So, those are some of the issues in this area that we've seen. These sub-grant award decisions and vendor selections must be accomplished using a fair and transparent process. Again, we just talked about that.

Consultants. They're a tricky one. With consultants, you should be asking yourself if and when you're going to hire a consultant. I like to tell grantees put on the investigator hat and you should be asking yourself the who, what, when, where, and why. Who am I going to hire? Who am I bringing on as a consultant? Why are we bringing this individual on as a consultant? Is there someone within our organization that already has the skillset, right? When we do we plan to bring them on? How are we going to bring them on? What does that look like? So, you should be asking yourself that question when you're thinking about bringing on a consultant, because that will help you alleviate a lot of potential issues if you're asking yourself those questions instead of just bringing someone on. So, with CY, excuse me, with cheating – I always give the acronym CYA. I always give this acronym. CYA. No need to post it in the chat. Everyone knows what CYA means. Can you articulate? Can you articulate why you selected this vendor over another? Can you articulate why you decided to sub-grant funds to Rob Ransom, your brother? Can you articulate it? Have you made OVW representatives aware of something that you plan to do, because that's a requirement, too. If you think that there's a potential conflict of interest, you need to make the government aware of that, okay? So, again, CYA – can you articulate?

So, I'll talk about this investigation. As you see, the government awarded a grant to a non-profit organization, which in essence turn over the award funds and program responsibilities to a for-profit entity. So, essentially, you had an organization that was eligible to receive grant funds, and they turned the funds over to an organization that is ineligible or was ineligible, in this particular case. It's conflict of interest.

This particular case here was worked by a former colleague of mine with the Department of Health and Human Services OIG. And I include this one because I want you all to pay close attention to the sentence was imposed in this particular case. This

individual was sentenced to 18 years in prison and ordered to pay \$13.5 million of restitution. Now, this was one of the loftier sentences I've seen for a grant fraud case. But, again, I have to show you grant fraud can carry significant penalties. I want you all to be aware of that, and be cognizant of that, as you're dealing with grant funds. This particular case shows how grant fraud can be widespread, and it doesn't stop at a certain level. Where in this particular case, an elected official was ordered to serve nine and a half years in prison for grant fraud. So, it can happen. It can happen.

Which brings me to the next full question, and I'm not sure if I have a poll for this one. But, again, just going back to what I mentioned earlier about consultants and some of the questions you should be asking yourself if and when you want to hire a consultant. The who, what, when, where, why, how much. You should be asking yourself these questions when you're thinking about hiring a consultant. And now, I'm going to turn it over to Special Agent Robert Ransom, who's going to talk about stealing, which is easily the largest risk you'll have to deal with and is the one we see the most of. But I'm going to turn it over to Rob. So, thank you.

ROBERT RANSOM JR.: Awesome. Awesome. Thank you so much, Jeremy. I appreciate that. As Jeremy stated before, keep in mind, fraud, waste, and abuse as we go through this part of the presentation. So, when you think of stealing, you think of the action or offense of taking someone else's property without the intent of returning it. Basically theft. So, if you could hit the next slide for me, Jeremy. Okay.

When you think of theft and you think of individuals that engage in fraud, waste, and abuse, here are just some traits, a few examples that you all should be aware of, and be on the lookout for when it comes to dealing with fraud, waste, and abuse. Sometimes they are very smart, bold, creative, organized, well-liked. One of the biggest things is manipulative, because a lot of people, when you talk about fraud, waste, and abuse, they like to manipulate things to work in their favor, or align in their favor, so that they can perpetuate the offense or perpetuate the abuse when it comes to getting funding. And when you talk about money, that's the first thing that I usually think of is someone manipulating others, or a system in order to benefit themselves. If you could drop to the next slide, Jeremy.

All right. Awesome. So, these next few slides, we're going to highlight just a few case examples, as Jeremy stated, that highlight the fraud, waste, and abuse. So, first we have embezzlement, and I took a couple notes here. I highlighted things that I wanted you all to really take heed to. A former Finance and Operations Manager for the Wisconsin Coalition Against Sexual Assault pled guilty to charges of embezzlement.



This individual embezzled approximately 50 grand from a DOJ OVW grant. That was one thing I highlighted. And as Jeremy stated in his earlier part of the presentation, the penalties range from probation – three years of probation – ten months of home confinement, and restitution. So, you have to ask yourself, if this is worth it. Is this amount of money that I'm thinking of stealing or committing theft, is it worth three years of my life, millions of dollars of restitution or fines? So, you really have to think about that. The long run. That's why it pays to just be straight up and have everything aligned to where there's no question when it comes to our desk, because, again, as Jeremy said, we will find out and a paper trail is easy to figure out. You can only be slick for so long before you will get caught. So, if you could flip to next slide – which would be using grant funds for personal gain.

As I said before, you know, a sentence of 2.5 years in prison in order to pay over \$400,000 in restitution for unauthorized payments on personal credit cards and cell phones over a five-year period, that's just – I hate to say it in plain words – but that's stupid. That you would do that with grant funding that's supposed to be helping and advocating for other individuals, but you're using it for personal gain. So, as stated before, outright stealing can be bold, as you can see in this example here, for using grant funds for personal gain. As we go to the next slide, which talks about a case where – a charter school theft – where an individual stole \$3 million from several charter schools by creating fake companies and funnelling school funds. This goes back to that creative mindset and manipulative mindset of individuals that steal. And this is just how sophisticated certain grantees can be when it comes to fraud, creating LLCs, generating fake receipts, fake invoices, moving money around, creating multiple accounts to move that money that they're stealing, so that it makes it very convoluted when it comes to us, as far as investigating. And, again, as I said before, you want to think, is it worth it? At the end of the day, is it worth it? Because I can tell you right now, it's not. So, as we hit to the next slide, which is showing – this is just some examples of receipts that can be generated from sites that can create like expenditure requests.

So, the next slide will show – okay. Thank you, Jeremy. I appreciate that. So, this site is no longer active, but it's sites like this that exist to generate fraudulent receipts to disguise fraud as legitimate. With this specific website, you could put in any given number and it will generate an expense report that you could therefore turn in to say, "Well, these were all my expenses that were covered with the money that was allocated to me for whatever reason." So, this goes back to that creative mindset of fraudsters when it comes to moving money and theft. Next slide for me, Jeremy.

Let's just name some common ways people steal funds. You have credit and debit cards, which I call "in your face" type of fraud, as seen in some of the earlier case

examples. With the paying for a phone bill and personal expenses for over five years. That's in your face, like deliberate. You have payroll manipulation, that would be considered cooking the books, where you're able to use Quicken or QuickBooks to hide doctor expenses so that it somewhat jives with money that's being spent. You have collusion with a vendor, which is number three, which falls under conspiracy and collusion, being something that you have to be aware of. I know Jeremy talked about that earlier in some earlier slides where he and I would have sidebar conversations, knowing good and well that this is how we're going to lay out the scheme. So, you get the money and I'll make the invoices and we'll start doing our pattern like that.

That brings us to our last poll question if I'm correct. So, internal controls are? Yeah, everybody's pretty unanimous on E. I think everybody is going to get themselves an agent badge. Will be certified investigators, man. And that's correct. Internal controls are basically an important way to mitigate risk, fraud, waste, and abuse. When we talk about grant fraud prevention, these are just some of the things that we just want you to be aware of. And, as Jeremy said, we're not trying to make you all special agents in the course of two hours, but internal controls matter. Familiarize, and read the agreements and documentation. This is a big thing. Due diligence is an ongoing responsibility. It doesn't happen just at the pre-award phase, or the post-award phase, or while you have the money. It's ongoing because you don't want to get into situations as some of those case examples. You want to ensure all applications, financial certifications, and drawdowns are accurate and progress reports are turned in on time. You don't want to get into the habit of turning progress reports and documentation in late, because a lot of times that may raise the red flag. And you don't want to draw that attention to yourself. If in doubt, ask the grantor or an outside expert. That's pretty self-explanatory. And facilitate in internal dialogue, which goes along with that internal control because you want to make sure that there's no question, when you receive funding, that there's misappropriation and fraud, waste, and abuse that occurs. So, just some things to keep in mind.

There're some other things to remember. You want to communicate with your OVW representative. That's very, very imperative. Utilize the guidance provided online from the grants guide, online training. Make sure you stay current with your training and when you have training, actually take the time to look and retain the information. And this is actually a very important thing as well. Grant funds are awarded for a specific purpose. And you see "specific" is highlighted in red because when you get the funding, you are to know that it is assigned for a specific reason, and if you deviate from that reason, then you start to get into that red area. You want to make sure you stay aligned with what the funding is set to be used for. So, a question that I just want you to think about, as you've heard is, "What are some fraud risks your organization may

encounter?" That's a question you ask yourself, that you may encounter, that you have encountered, or some things that you might possibly encounter in the future now that you know what to look for, you know a little bit about fraud, waste, and abuse, how theft occurs, how it's manipulated, and how collusion occurs. That's something that you need to think about – what fraud risks your organization may encounter. And I think that is it.

PARTICIPANT: I have a question. I've been in coalition work since 2007. I've also heard, while visiting different grantees doing TA work, and some of the things that I have heard of were disgruntled employees or disgruntled community members calling the grant and fraud waste on either the programs or coalition – any entity that they worked with and doing almost like false reports. Is that a common thing that has happened? In my fifteen years of doing this, this is something that I've heard at least three times of somebody making false reports or getting the attention. Now, granted, if you start working and you need to and you see some red flags on your end, of course, you're going to investigate. But I just wanted to know a little bit more about that because I've heard that as almost like a retaliation amongst the community. And I've been very curious about how that impacts and how does that waste your organization's time supporting that kind of work.

JEREMY JEFFERSON: Sure. Sure. Thank you. Thank you so much for your question. So, I'll say that when we receive a complaint, as agents, as investigators, we vet those complaints. We do interviews. We may look at documentation. So, it's one of those things where we don't necessarily have a visibility in terms of what may be just a disgruntled employee and what may be a legitimate complaint. From our perspective, we approach those investigations all in the same way. We vet the complaint, we conduct interviews, and do what's necessary, because, again, from our perspective, we're getting it on the backend. We're not privy to information or a disgruntled employee or what have you. And there have been times where we found that to be the case, but, again, we approach every complaint the same, and we have a very thorough vetting process, interviewing, things of that nature. It's just hard for us, on the frontend, to just rule it out and say, "Oh, this is a disgruntled employee or a disgruntled community member." And, Rob, I don't know if you want to add anything to that.

ROBERT RANSOM JR.: Yeah. Yes, I actually do want to add. Guadalupe, that was a great question. And I just want to say that it's never a waste of time, because that's our job – to investigate. And we see that often. Not as often as other OIGs, but when you have multiple businesses or multiple agencies doing the same work, it becomes

competitive, and it happens. But, again, it's not a waste of our time because that's what we get paid for, to investigate and get down to the bottom of things. Again, as Jeremy said, that's what we do. If we find that there's nothing there, then there's nothing there. But eventually, we get down to the bottom of it, so...

JEREMY JEFFERSON: Thanks, Rob. So, we have a question in the chat. It says, "What should we do if a disgruntled employee destroys evidence, and you go to ask questions and the grantee under review says they don't have?" Thank you so much for raising that question. I would say, again, going back to one of the slides, communicate. Communicate, communicate, communicate. Communicate with your OVW representative and say, "Hey, I had Jeremy on staff. He destroyed a bunch of paper. He destroyed a bunch of receipts, documents. He's disgruntled." I would communicate that early on, and say, "Hey, this is what happened," just so there's a paper trail, but I would say definitely communicate then. Just communicate it.

ROBERT RANSOM JR.: And I see another question. "Are there any general best practices for internal controls that you've seen?" They vary. Which is a good question. They do vary. And I usually tell people this. You want to be detective and preventative rather than corrective. You would like to detect it and prevent it at the frontend instead of trying to be reactive. So, it's important to have like communication, you know, amongst each other, amongst your staff, and let them know, you know, to familiarize themselves – as we stated in the presentation – to familiarize themselves with what the money is supposed to be used for, the guidelines, and to ensure that they take the trainings and turn in the documentation and reports on a timely manner so, like I said, it doesn't raise a red flag.

JEREMY JEFFERSON: And we have looks like another question. "At what point does the OIG get involved? Do the grant administrative agencies call you and when we find that fraud is or might be happening?" It varies, right? It varies. We've gotten involved at many different points, whether the fraud has already occurred, maybe someone is aware of something that's going on. That kind of varies, so I can't give you a solid answer as to when we get involved. And we receive calls from a lot of different sources, so...

ROBERT RANSOM JR.: I see, "As a funding administrator, what's the best way to handle if you are suspicious of a sub-recipient and/or misusing funding or falsifying

documentation without solid proof?" There's nothing wrong with submitting a report or submitting a complaint. Again, that's what we get paid to do. If your gut is telling you something's wrong and it's raising some red flags with the way that they're moving and their practices, I would say, don't let it keep going on. I would report it just to cover all bases.

JEREMY JEFFERSON: Right. And to add to that, Rob, I would say, begin documenting your interactions with that particular sub-recipient. If you have that inkling that something may be going on, begin documenting because that will help us if and when you do file a complaint to start our investigation. If you have some notes or things that say, "Hey, I interacted with this subrecipient on the 2nd of February. This is what I asked them, and this is what they provided." So, I would say, definitely document that. As Ron mentioned, it doesn't hurt to file a complaint, if you feel that's necessary. Looks like there's one more question. "Can you require the sub-grantees to not destroy financial records, and if they do, it's a breach of contract?" I'm not sure how to answer that. Tamika, if you wanted to come on mic and provide a little bit of context.

TAMIKA: Hello. Yeah, my question was more for the questions around the sub-awards. Like, can't it be required as a part of your MOU or your contract that they cannot destroy financial records or that the sub-award can be ended?

JEREMY JEFFERSON: Yeah, that's a great question. I would pose that to your OVW rep and ask them for specifics, but that's a great question. Unfortunately, I'm not the person to answer that. I think that's more of a question for your OVW rep. We thank you so much for your time. And if you have any additional follow up questions, again, Rob posted his information in the chat. Feel free to reach out to Rob and/or myself. We work in teams. So, again, thank you so much for your time.