Fox Rothschild Podcast

The Presumption of Innocence

Episode 38: A Blueprint for Compliance: The Fraud Pentagon Theory

Featuring Matt Adams of Fox Rothschild and Nicole Slinger and Jonathan Marks of BDO

Adams: Hi, everyone, and welcome to "The Presumption of Innocence," a podcast brought to you by the White-Collar Criminal Defense and Regulatory Compliance Practice at Fox Rothschild. I'm your host, Matt Adams.

And today we have two fantastic guests, both CPAs with the global accounting and consulting firm BDO. We have Nicole Sliger. We also have Jonathan Marks. And today we're talking about keeping an organization compliant. A lot of what we talk about here on "The Presumption of Innocence" really has to do with reactive and policy. Big picture stuff when it comes to the white-collar criminal defense and regulatory compliance world.

But today I wanted to shift our focus just a little bit into keeping a compliant business. And in particular, a business in a highly regulated environment, such as financial services -- where I know our two guests have extensive experience -- and other regulated environments, like publicly traded companies and health care.

We need to focus, for this discussion today, on the proactive steps that can be taken to eliminate those knocks at the door, those problems with subpoenas and civil investigative demands that we frequently discuss, and really get into the nuts and bolts of proactive approaches to eliminating compliance issues on the front end.

And I'm fascinated by a concept that our guests today have developed. And that is a concept called the Fraud Pentagon. And just briefly, Jonathan, I've heard of the Fraud Triangle. What's the Fraud Pentagon, and how did this come to be?

Marks: Thanks, Matt. Well, the Fraud Pentagon came to be -- I, much like Nicole, this has been my life in forensics. And so the way it actually came to be: I was watching a "Frontline" program, if you guys remember "Frontline," and it was titled "How to Steal $500 Million." And the episode delved into a story about a former president of a now defunct nationwide retail chain specializing in discounted drugs and groceries.

And it was revealed that the former president, along with the company's CFO, conspired to conceal the company's financial losses by manipulating the financial records. So, among numerous lessons that should be gleaned from that show that I watched was the one that most resonated with me and appeared to be conspicuously evident or hidden in plain sight-- it was the conduct exhibited by the CEO or the leader of the company. And given the understanding that fraud involves not just

obstruction, but also deflection, deception and distraction, I became sure that the human element had been overlooked. And shortly after this headline scandal, a series of other high profile corporate scandals emerge, including the famous fraud cases, which we can go on and on and on about.

But it was really what happened in December of 2008, and then was really solidified in my mind in 2009, and that was the Madoff actions. And those really served as a catalyst for me personally, and an inspiration for me to take some type of action. And so, the way it all kind of came down was, I pondered the question is, how this oversight occurred?

So I literally ran to the supply room and grabbed a bunch of dry erase markers and a giant whiteboard and I started writing. And from this exercise, I reached a conclusion that Cressey's Fraud Triangle -- actually, he didn't even invent the phraseology Fraud Triangle, that was that came later. But his theory regarding the three essential components required for occupational fraud were pressure, opportunity and rationalization. Those made perfect sense to me. And you got to remember, Cressey's study, you know, "Other People's Money," was really in the 1950s. Businesses and people acted a little bit different then, we're talking, you know, 2008, 2009. And so, um, you know, I looked and I said, "What's missing?" And the missing pieces to me were this concept I label perceived competence and arrogance.

I also thought, in practice, that many ignored the human element of fraud, hence, I developed the Fraud Pentagon. And use the Fraud Pentagon as a mechanism for me -- and I was teaching it to others -- when we were looking at potential alleged frauds and gatekeepers of white-collar crime as to those types of behaviors, you know, that might be there that would be indicative of something that was really not wrong. So that's really how it all came to be.

Adams: And listeners of our podcast will recall, just a few episodes ago we had Eugene Soltes, professor at the Harvard Business School and author of "Why They Do It: Inside the Mind of the White-Collar Criminal" on our program. And Professor Soltes had perhaps not as direct and succinct a way of looking at this human component. But he really dived in from an academic perspective on what it is and why it is that drive individuals within an organization to sort of veer off course and detour into what I would call noncompliant behaviors that are both an organizational risk and a potential risk to them individually.

In practice, how do you use this Fraud Pentagon that you've developed to root out noncompliant behaviors within an organization or instruct organizations on how they can be more compliant?

Marks: So, in practice, I think you can use it a couple of different ways. One is, again, if you're focusing on or developing a fraud risk assessment -- and we're talking about, you know, sort of proactive things, which, you know, your preamble with regards to today's show is, you know, how do you get in front of all this? So, if you're doing a fraud risk assessment, the biggest thing in practice is not only identifying the act, the concealment and the conversion.

So, the act or the fraud schemes you know, the concealment was, how could the fraud potentially be concealed? And the conversion is, how could one individual or a group of individuals take what they

were doing and convert those ill-gotten gains for their own personal reasons? As part of all of that, as you move through the exercise, one of the key things that I look at -- and I know that we look at in practice -- is who are the gatekeepers?

You know, and for a long time, there was sort of this taboo about actually looking at individuals because everybody thought we were stereotyping them. When, in fact, that's not what we were doing. We were actually profiling them. And so when you're profiling an individual, there's a bunch of different things that go into this. And so, the elements that we mentioned before, you know, pressure, opportunity, rationalization, competence -- or perceived competence -- and arrogance. If you looked at that particular individual, and you looked at those particular elements, you could determine from a risk perspective, rather, some of that risk may or may not be there. And so, again, from a proactive perspective, now we can go and we could design controls or make sure that controls are in place to potentially thwart that behavior.

Now, the interesting part of all of this is that the pentagon really looks at the perpetrator. Then if you look at the triangle of fraud action, which is on the other side of the equation, that really looks at the crime.

And the Triangle of Fraud action is something that most people really don't understand. And those are the three elements of an actual fraud, which I had mentioned, were the act, the concealment, the conversion. So, now, you know why we go back and we mentioned the fraud risk assessment, because those are key elements in an assessment. And the gushy thing in the middle that thwarts that perpetrator from actually committing the crime are internal controls.

And so, this is how we could potentially use this in practice is to visualize all this and look for potential risks within the ecosystem and design controls that are much more effective in thwarting that potential behavior. And what I mean by being effective, I mean, that they actually meet that particular objective. And also, they try to -- not all instances is this possible -- but they try to quell, override or circumvention. And I know Nicole has seen this before, so I'm kind of interested in her twist on all of this as well.

Adams: Yeah, Nicole, I was just going to jump to you, because we're really taking a behavioral science look, in a way, at compliance. And in particular, this pressure, opportunity, rationalization triangle, and then adding this competence and arrogance.

Talk to me about competence and arrogance. How have you seen that shape the compliance landscape of the organizations that you've worked in as a consultant over all these years?

Sliger: Yeah, I feel that the human element really comes into play. I mean, we're all humans, right? We're part of an ecosystem of a company with a culture. And I think an individual's persona of themselves really does feed into what they do day-to-day and how they justify their reactions and their actions during the workday.

So, you know, we've seen a lot of interesting characters over the years as clients and as potential perpetrators. And really just how they come to the table and, interact, you know, day-to-day, you know, does tell a lot of what their past misdoings may be.

Adams: And how do you, control the competence of your individuals? Is that really a top-down approach? Or is that a bottom-up approach? Because if we think about competence as the individuals within your organization's ability to actually carry things out with a level of competence, so they're not hiding things, they're not going down the path of trying to cover up for errors and in the process, creating a compliance risk. How do you ensure compliance through competence?

Sliger: I feel you have to have a very good vetting process, you know, employment, recruiting. You know, making sure that you're hiring qualified individuals that have the necessary skill sets to work in the accounting department or finance department, whatever department we're talking about. And really vetting those references, doing a background check, making sure that we get the supporting documentation for those qualifications.

I mean, I think we've seen times where, you know, the resume just isn't what you get in reality and that is, you know, part of the issue when these things come to fruition.

Adams: And Jonathan, if arrogance can tend to be a driver of fraud or noncompliant conduct within an organization under the rubric of your Fraud Pentagon, how, how do you police arrogance?

It's such a internal, human, individualized characteristic that it's really tough to combat, isn't it?

Marks: I think it goes both ways. And I think this is where, you know, you have to be really in tune with what's going on within your organization. I know we mentioned the word culture before, but, you know, culture plays a big part of this.

For example, you know, if you have a leadership style or a culture where you're encouraging people to be participative, you know, and building consensus, and then all of a sudden you start to cut them off, these are the types of red flags that we would pick up on -- or we would find out from doing an investigation -- that may have led to sort of the root cause of the potential bad behavior and misbehavior. So, it's not easy. We're not psychologists, but, you know, we play the role of psychologists sometimes.

I always say, people always say, well, what makes a good forensic accountant? And Nicole, you could chime in here too, but you have to be a good auditor. You have to understand the legal system. You have to be a little bit of a good psychologist, so to speak, you know, and a counselor. Good listener, good analytics. And, you know I'm sure Nicole could pick up on this, but a lot of times we are playing into that and we're trying to get in the mind behind the crime, so to speak, to understand what that individual may or may have not have been thinking. And, you know, sometimes it's way too late, but a lot of times there are red flags. And I think, you know, if we want to get into that, we can kind of get into what those particular red flags might be in advance.

But like I said, when we do investigations, Nicole, if we start to look at emails or communications and someone says, " Don't worry about it, no, one will ever know." Or, you know, "Let's take this conversation offline." Those would be red flags to somebody.

And then the ethics comes in. You know, the individuals on the other side that start to see this, do they have the courage to speak up and say something? Because if they don't, then it's too late.

Adams: Yeah, and this is such a uniquely human kind of inquiry. We often are in the position on the legal side to go into a government, to go into a regulator and say, "There is a culture of compliance at this company."

It's a key phrase that we use frequently in these investigations. And oftentimes, we are rebutted by data, evidence that suggests the contrary. When you are looking at these uniquely human characteristics as sort of the red flags for issues with compliance, I'm really interested on how you help your clients devise internal controls that hit these touch points. And Nicole, let's, take them one by one, and I'll, if I may, I'm going to sort of pepper both of you with questions about these internal control type issues.

Let's take competence first. Nicole, you've been talking early on about ensuring competence by vetting your employees. By making sure that there's checks and balances, so to speak, on their work product. But is that the only types of internal controls you can place to ensure competence? I harken back on the educational system in our country. Standardized testing has really taken over as sort of the benchmark for internal controls on the educational system. And for good, bad, or we don't have to debate that here, but those standardized tests tend to be used to evaluate whether a particular school district is doing well, or doing poor. In fact, in many school districts, your ability to secure funding is based on those standardized testing scores. And a lot of weight is based on that. In a workplace, especially a highly regulated workplace, is there an equivalent Nicole, in your experience of that standardized tests that can serve as the litmus test for competence? Or is it more of a holistic thing?

Sliger: I think it's the latter. Matt, I think, you know, what really, in terms of competence, be able to monitor that internally. You have to have a good segregation of duties within the organization so that there are, to your point, checks and balances that are in place that, you know, prevents or hopefully can detect if there is an issue. You know, someone coming along and having to re-perform their work. If you need to take mandatory vacation so that something can clear the system and be discovered if there is something awry. So I think there is a holistic approach and you have to have mechanisms in place so that you have a reviewer of certain individuals' work if they're in a key role like that, that could be subject to manipulation.

Adams: And we've seen this in the financial services markets where we have mandatory vacation periods, two weeks out of the office, you're not able to log in. You're not able to access your emails. Nicole, when those types of things happen, what are we looking for from the organizational perspective? You know, now we have mandatory two weeks vacation and frankly, I wish they did that in the legal services market because I would appreciate that.

But, you know, mandatory two weeks, you're out. What is it that you as the consultant, the accounting professional that's retained in by the firm to go in and look at these things, what are you looking for during that period of two weeks out of the office with no access?

Sliger: So, maybe I'll answer that with a story of a case that I worked when I first came to BDO from the Big 4. It was a metals manufacturing plant in the South and the fraudster was the controller. And he was always buying the accounting department lavish meals and treating them to concert tickets.

And funny part about this case is it all started out as an HR issue, right? It was a sexual harassment claim. Turns out he was sleeping with the AR clerk and then after they broke up, you know, he continued to pursue her. So, after he was suspended, that's when this all came about, because he had been hiding his cash misappropriation and got lazy and did not reconcile the bank statements. And so, in a hail Mary attempt to cover up his tracks, he came to the AP clerk and ask them to file away some of the reconciliations. Obviously, the AP clerk, you know, was in the right mind and thought that was odd and kicked it up to the CFO for an investigation. But because he had been out of the office for a couple of weeks, he had gotten lazy and been doing this for years, you know, he realized that there was an issue. So, long story short, to answer your question, you know, that's what you're looking. You're looking for something in those two weeks to hit the ledger or not be done. Right? And that would alert someone to, "Oh, what happened here?"

Adams: And Jonathan, I'm going to pose the same question to you, but with the other variable that we were exploring a little bit ago, arrogance. You know, we talked about a culture of compliance. As I see arrogance in one of these regulated industries, where these compliance issues may tend to pop up, I see arrogance is being principally a cultural issue. So how do you put internal controls in the classic sense, right? This is not classic CPA work here, you're playing bubble gum psychologist, in a sense. How do you put internal controls around arrogance as one of your Fraud Pentagon variables to ensure a culture of compliance?

Marks: So, let's go back to what arrogance really is, and that is this sense of entitlement or greed or hubris on the part of an individual, right? And so, one of the things that I've learned is the 10-80-10 theory. And that's, 10% of the people in an organization are ethical, 80% are situationally ethical and 10% are committing fraud all the time. So you can't control a human.

Adams: That's a pretty stark picture, Jonathan.

Marks: It is, and you've got to remember that it's just a theory. It's not an absolute. But if you think about it for a second and you really unpacked your question, you know, how do you control that individual? I think the way that you do that is you try to control what you control. Control the controllable. So, if 80% are situationally ethical, and you can control them by making sure that there's a good culture and that people are listened to, and there is no retaliation for people speaking up, and things like that, then they won't cross over into that dark side, so to speak.

And so now, instead of having 80% that are situationally ethical, if you can get them to kind of tilt towards the more ethical side in all instances, and you know, you already have 10% of the people

that are already ethical, let's hope that that 90% can ring fence in that one individual to some degree and make sure that that arrogance is somewhat contained.

And so --

Adams: Give me an example. Give me an example of an internal control in an organization that would be a checking force on this arrogance variable.

Marks: Four-eyes principle. So you have somebody who's a gatekeeper that makes decisions. Their two eyes are the ones that make that decision. It's not a unilateral decision. It has to go to somebody else before it actually meanders its way to being signed off on. And so, you know, I think that's really a great way of kind of putting that in check. If somebody knows that they have ultimate authority and they're in that realm of the 10% of the wrongdoers, so to speak, that just creates havoc.

But if you can create a four-eyes principle where decisions are not unilaterally made, that somebody else is signing off on that, I think that tends to kind of back off somebody from thinking that they can get away with anything that they want.

Adams: Yeah, it's a really fascinating that we're having these discussions because when we think about a culture of compliance my mind immediately goes -- and my audience will know, we frequently talk about the Department of Justice's Principles of Corporate Prosecution. And oftentimes that becomes a mini exercise in trying to prove -- or demonstrate with objective evidence in some way, shape or form -- that you are a compliant organization, and maybe one or two bad actors, you know, human nature being what they are. And therefore you shouldn't punish the whole because of just a few bad apples.

And I think this is really telling in terms of the types of things that, as a legal team, we would be looking to highlight. And on the front end, implementing some of these strategies really does help us and bring it top of mind when it comes to the inevitable. When there is a problem in the organization and the organization itself is potentially jeopardized by those few bad actors. And I'm fascinated by the conscious discussion that we're having around these topics.

But lest we forget about the original triangle: the pressure, the opportunity and the rationalization. Let's go back there for a second. You know, Nicole, how does pressure play into a compliant organization? How is the concept of this, again, uniquely human condition that we all face, how do we put controls around that?

Sliger: Yeah, I mean, that that's a hard one, right? Because pressure is just present. To Jonathan's point, control what's in the controllable. So, I mean, we all have our own financial pressures, whatever pressures to succeed. And, you know, it's just not something, I don't think you can create an internal control around. But you can be cognizant of it and you could do periodic background checks on your employees to understand if there are any evidence from the public record that might suggest there are undue pressures. You know, I don't think that's something that you can solve for within internal controls. But I guess, just being aware of the possibility and, when combined with one of

those, the other elements, right, opportunity and rationalization, that's when it all comes together and people can justify their actions.

Adams: And building that one step further, I mean, we really are taking -- you both are CPAs by training your background is in financial controls -- but we're really injecting a sociological, a psychological bent on those traditional concepts of internal controls. And I'll kick it to you, Jonathan, on this other variable, the rationalization component. Where is it in an organization that you can police this variable towards the goal of building a more compliant company?

Marks: Again, you know, sort of taking a look at what that actually means, like, rationalizing why somebody would be doing something ex post facto. So, in other words, after they commit the bad act, all of a sudden they sit back and they go, well, you know, maybe I deserve that. Or, I wasn't being treated fairly, so, you know, I'm fighting back, you know. How do you control stuff like that? And even talking about sort of the competence piece a little bit as well. And then I'm going to get back to your bad apple scenario in a second and tie it all together.

I think we live in a world right now where fraud has become more of a team sport. And I think the regulators have figured that out. So, it's no longer the bad apple. It's the bad apple, it's the bad bunch, it's the bad crop. It's the ABC theory of fraud. You have a bad apple, you have a bad bunch, which creates a bad crop. And that's where I think the regulators are really heading.

With regards to competence and with regards to rationalization, I think it really comes down to culture. And I think it does come down to the human element. In one way, I think, maybe corporations -- and not all corporations or organizations can do this, but, you know -- one of the things that Cressey talked about when he created his original three elements was shareable and non-shareable type of situations. And so, we talked about pressure before -- pressure being exerted at home. I have three kids now going to college. Does that exert pressure on me? Yes. If it does, then how do you alleviate that pressure? Maybe I'm not making enough money, you know, maybe the reason that I'm committing these bad acts is because I need to pay for my kids' tuition.

So, I think we live in a world right now where we're just not listening enough. And I think the way that we can build controls and even prevent to some degree -- and I don't even like using the word prevent or deter -- people from committing bad acts is really trying to defuse the issue. And the way we defuse the issue is by helping them.

So, one of the things that I thought of when I came up with the Fraud Pentagon way back when, was what if we had a department within the company? It could have been -- and way back then, they called it human resources, now they call it people services -- but, you know, maybe the company put away a little bit of money to help those that were going through these pressure-packed events. Maybe they had some type of un-shareable type of thing going on. You know, for example, the college tuition thing, maybe they had some addiction problem that they were trying to get around. But they needed some cash and the way that they were getting around this was they were committing bad acts. Instead of doing that, if the company helped them and, you know, alleviated that pressure, then those bad acts may not even have occurred.

And sometimes these things start out very small and then they mushroom into things that are much, much larger. So, I don't know that you can look at one thing isolated by itself. I think that there is linkage amongst all of these things, you know, like pressure, opportunity, rationalization, competence and arrogance.

And, I think the way that, if we're going to really take this seriously and we're going to really try to stop people from doing things that potentially could be harmful to an organization, there are some things that, just, we may not be able to control. But some of the other frauds that happen -- the garden variety frauds, you know, the accounts payable frauds, or, you know, some of these other frauds -- at the middle level or the lower levels of organizations, I think a lot of that really comes back to training, education and listening, and trying to, like I said, diffuse those situations.

Adams: I don't want to not touch on opportunity, but I saved it for last intentionally. To me, opportunity seems like the classic accounting internal control. It sounds to me like the classic, we need to have processes in place where there are checks, where there are balances. Where there are guard rails to ensure that no one person can sort of take over the joint, so to speak, without somebody else finding out. Nicole, would you agree with me?

Sliger: Yeah. Yeah. It goes back to what I was saying earlier about having the segregation of duties and just the environment there, which, you hope you have some preventative triggers in place that would signal that something was awry. So definitely agree with you there, Matt.

Adams: Now bringing it all full circle, right? We've really designed sort of a psycho-social profile of bad actors, groups of bad actors within an organization. Are you saying, Jonathan, with your Fraud Pentagon theory that you really do have to have a pulse on the psycho-social components of your organization in order to be compliant?

Marks: I believe that you do. I think there has to be some level of component there. Because, again, going back to what I said earlier on, when you look at a fraud, you know, the obstruction, the deception, deflection and distraction, white-collar criminals try to build a false sense of integrity around themselves because they want you to trust them.

And when you trust them, you lower your level of skepticism. And that's just inherent in human beings. In Nicole's situation, the story that she described where the individual was trying to literally bribe them, you know, with concert tickets or candies or goodies or whatever, the reason that they're doing that is because they want you to like them.

And when you like them, again, you're building this false sense of integrity around yourself. And some people, they can't help themselves and they do lower their level of skepticism. So I think, going back to what you asked, Matt, if you don't have that, and you don't have that self-awareness and you can't calibrate that trigger that keeps your skepticism at the proper level, I think a lot of times we miss stuff. And, that's one of the things that we work very, very hard, you know, through training and education and through quality control, to make sure that that absolutely doesn't happen.

Adams: Well, let's build on that. So now we've really established the foundational components of the Fraud Pentagon. And now we want to put that into action. So, Nicole, talk to us a little bit about some of the day-to-day controls that you help organizations put into place to eliminate these risks that come from this five-prong monster that Jonathan has devised and we've been talking about for the last little while here.

Sliger: Yeah, and I think it all ties back to education and making employees aware of potential noncompliance issues that can happen, and building a culture where there is comfort in speaking up. You know, hindsight's always 2020, right? You know, everyone, when a fraud becomes known to the company: "I knew that, you know, that was always odd that he did this," or, "you know, I always thought something was off." And, you know, I think building an educational program, self-awareness of that professional skepticism, right? And having the confidence to report something if something seems awry, I think is really important. So, training courses on, risk management and just behavioral science in general. And understanding that conscious and unconscious bias that might be there. And again, just building on the level of culture where it is okay to speak up and individuals won't be retaliated against.

Marks: Yeah, and can I just expand on that for one second? Because Nicole, those are awesome points. You know, I think one of the things we try to do as a practice is, when we do provide training to our clients and to others is, training is a very interesting animal because if you don't train people the right way then you have this concept called "disremember risk." And there's studies that say that 90% of what you learn during a training exercise is forgotten within a week.

One of the ways to combat that is to really emphasize during the training, those things, those triggers, as Nicole was saying. So, for example, red flags. If I walked into a training session and somebody was talking about the Foreign Corrupt Practices Act and they told me it was enacted in 1977 and got into the whole history of it, I don't know that I'd pay attention. But if somebody told me that there are these specific red flags -- data, documents, lack of controls on behavior -- gave me absolute specifics on what to look for, now I can walk out of that training and say, "You know what? I have something that's actionable here, not just something that's theoretical."

And so that's one of the things I know we strive for as a practice and as a firm is to make sure that we're doing that and we're emphasizing those types of things when we do our work and we do our training. There's a big difference between training and proper training.

Adams: All right, I'm going to put you both on the spot here with a short question, and I want a short answer. In one sentence or less, Nicole, what is the most critical component to an organization's internal controls to mitigate against the risks associated with the five-headed monster, the Fraud Pentagon?

Sliger: I have to say it's a strong accounting and finance department with qualified resources.

Adams: Jonathan, same question to you. In one sentence or less, how do you most effectively mitigate against the risks presented to an organization by the Fraud Pentagon?

Marks: I think it's what Nicole said, but I'll add to that and I will tell you that it's a very strong and surgical tone and conduct from the top that resonates down and through the organization. That messaging, walking the walk and talking to talk, I think goes a long way.

Adams: To that point. Nicole. what is an example of a weak accounting and financial department that would present risk to an organization? How do, you know when you see that, organizationally?

Sliger: You may not have a very robust department, right? So you only have a limited number of resources that are allocated. And by default, that means that people in that department are wearing many hats. And so that whole premise of segregation of duties goes out the window. So, that is one example there.

Adams: All right, so let's, go down the path of sort of seeing how this plays in action. Now, Jonathan, share your thoughts for us on applying your Fraud Pentagon, what I'm calling the five-headed monster, to specific fraud cases.

Maybe perhaps one of those famous frauds you mentioned earlier that have really become a household name for many of us. And as we've talked about on this program, many, many times, really dominated the headlines in the early 2000s when we saw sort of the high watermark of corporate prosecution.

Marks: What I do is -- I do this with every investigation. I'm a visual person, so I have my Pentagon on the left-hand side, which represents the potential or the alleged bad actors on the left. And on the right-hand side, I have the Triangle of Fraud action. So, I have the perpetrator and the crime. And so the way I actually put it into action, from an investigative perspective, is while I'm designing my procedures to do my investigations, I'm being cognizant and aware of those specific elements, those specific behaviors, those specific red flags and triggers. Along with, when I'm analyzing controls, are there weak or nonexistent controls?

So, in other words, it's not only analyzing the perpetrator, but that path for the perpetrator to get to the crime, which are the internal controls. I'm also analyzing those roads or those avenues or those bridges, to get to the particular alleged crime. That's what I do on the investigative side.

Flip that over, on the proactive side, like we talked about earlier on from, a fraud risk assessment perspective I want to make sure that if I can understand at least a little bit about the gatekeepers and the people that are instrumental and move in the organization, and understand how and what they're doing, and then look at the controls, I could then say, are those controls robust enough? Do they achieve the objectives that we're trying to achieve? What are the barriers, obstacles and hurdles that may be in place for our company to achieve those specific objectives? And then I look at the enemies of internal controls: compensation structures, time, the ability to override and so on and so forth. And I look at those and kind of marry that. And I think, like Nicole said before, we try to figure out the risk and the risk profile there. And that's how we really go about our day-to-day.

So, from a proactive side and a reactive side, it's really one and the same. And that's why I think it's not only training and education on our part, but it's also the experiences that we've had over our

careers that have -- you know, like Nicole talked about her particular situation when she first joined BDO, on that particular case. It's all those cases and it's the accumulation of all that knowledge over the years that really gets us to a point where we really can pull this all together.

Adams: And that's a great transition, because where I want to end today is I want to talk through some of the red flags you've seen in your career. Sort of the body of the top 10 list, so to speak, of the worst red flags that you saw, applying some of the theoretical concepts we've been discussing today into real life.

So, Nicole, let's start with you. I'm sure you've seen it all in your decades of practice, but give us a couple of examples of sort of the worst-case flags.

Sliger: Yeah, and I think it ties back to Jonathan's arrogance aspect of the Pentagon, when you have a CEO or CFO with a big ego. Primarily, you know, surrounded by some, you know, young'uns, or less experienced colleagues that may be naive or just not experienced yet in their career to be able to recognize some of the things that we're talking about today. Definitely seen that a lot, namely one case. This is going back several years ago. I actually think it was a "Law & Order" episode at some point. Jonathan's tying back to how these things become on the television screen.

Anyway, we were hired by counsel, as we typically are, to assist in defending the former CEO. This is a manufacturer again. And the fraud was earnings management where the company had been making its EPS targets by a penny or so each quarter. And the CEO's ego was larger than life, his clothes, his jewelry, his mode of transportation, with private jets, fancy cars, racehorses, you know. It just turned out that he wasn't just managing the company's earnings, but he had also commingled personal expenses into the business. And, you know, it's just, when you see someone that's larger than life, that itself should be a red flag.

And again, going back to hindsight being 2020. You know, if an individual within that organization at the time had saw this flashy individual, would they have maybe raised a hand and said, hey, something doesn't seem right here?

Adams: Is it an old-fashioned smell test?

Sliger: I think people know, right?

They just don't speak up and say something. They're like, that's none of my business, you know, I don't know, I don't trust my own judgment. And, you know, I think, I think if more people spoke up, we might have more work to do, right Jonathan?

Adams: Trust your gut. All right, Jonathan, the same question presented to you, now, about you know, what are some of the worst red flags that you've seen sort of, as you've deconstructed your Fraud Pentagon ex post facto in an effort to try to resolve some client's problem?

Marks: I think the worst I've ever seen was, I was in a board meeting while conducting an investigation and I was making a presentation to the board. And one of the board members said,

"Well, we needed to do this for the good of the company." And so, you know, sort of the big lie justifies unethical actions. And then the investigation stopped.

So, I mean, that was kind of interesting to me that the board was actually trying to protect the company and the unethical actions. And it said, like literally, this was done for the good of the company, you know, to keep the company going. And I think that's probably one situation that I personally experienced. I would imagine that that happens more often than not.

I think the other thing that I've heard a lot of is that, you know, we're going to innovate like no other company. We're going to do that at all costs. And, you know, I think there's a couple of recent cases where you can look at those and say, hey, those were giant red flags, and kind of interesting as to how that all kind of ties together. But I think if you look at those individuals today, we didn't even talk about those, but some of the recent cases that have come out over the last 24 or 36 months, those folks definitely would be case studies for the Mount Rushmore of the Fraud Pentagon.

Adams: The Mount Rushmore of the Fraud Pentagon. That is a, uh, that that definitely is an interesting way of putting it. I mean, my takeaway from this really is, again, we talk a lot about this idea of a culture of compliance. And I don't think there's one special sauce, to be honest with you.

I think that there's probably a pea soup of things that go into this. And in any given scenario, one issue or another, whether it's the private jets and the fancy modes of transportation, as you so eloquently put it, Nicole, or it's something else. I think most people have a guttural reaction and it is, I think, seldom a scenario in an organization where something comes to light and somebody somewhere doesn't pop up and say, yeah, you know, that never sat right with me. That didn't really fit in. And I always wondered about that. If we want people to blow the whistle earlier, so that these things don't metastasize, that they don't blow up and end up in some scandal.

Are you guys a fan of the whistleblower hotlines within the organization? Are you a fan of anonymous tips to the CEO? How is it that you implement a method by which people feel comfortable trusting their gut, evaluating these psycho -social variables that put their livelihood at risk, because they put their company risk. What's that single thread that you need to weave in order to make sure that those things get nipped in the bud, so to speak, at the early phases? Nicole, I'll go first to you and then get Jonathan's take.

Sliger: Yeah, Matt, I think you said it perfectly. It's the trust. Trust within the system, right? If people don't have faith that if they do raise their hand and report something up, that it's going to be thoroughly investigated, then they're risking their livelihood, as you said, with a lot of risk on their side and not much faith that something might be uncovered.

And so I really do think that having those reporting mechanisms in place where they're touted and communicated and everywhere, you know, on your, your banners, your screen savers, you know, really is important to make sure that if there is an issue that people feel comfortable. And a reward system, too, right, financial or otherwise, I really think that's key.

Adams: From, from your experience -- anonymizing the clients, of course -- but give me an example of how that works in real life, a very effective culture of reporting. When your gut tells you it's off, how you can be incentivized. All the conceptual things you just said. Give me a real-world example of how that plays out.

Sliger: Jonathan, you want to help me out here? I'm trying to think.

Marks: Yeah, Nicole, you and I've talked about this before. We do a lot of whistleblower work. And so, you know, how it really all plays out is -- we're in Philly, so I'll say, trust the process first, right? And then we'll kind of dip into this. You know, somebody sees something that, that's unethical. They realize that, they recognize that. And again, this is perfect world scenario. They've been to training so they know that if they look at data documents, lack of controls and behavior, they've identified a couple of red flags. They've done maybe their own mental gymnastics on how this is all going to play out.

They trust the process. And so, maybe they go to their manager, or maybe they pick up the hotline and they call. And, at the other end of that call, or the person that's receiving that, is listening to them, takes it seriously and then moves it to the next level.

So, you know, maybe there's an allegation review committee. Somebody reviews this and says, hey we need to investigate. And, obviously all those things should be looked at with the proper lens and the proper level of skepticism. And so, somebody investigates and they conduct a thorough and if, necessary, an independent investigation. All the time of communicating back to the particular individual, letting them know that we took their tip or their allegation or their complaint very seriously.

And at the end of the day, you know, whatever winds up happening, if there's bad behavior, there's organizational justice. So that individual knows that there's a beginning, middle and an end. And when people see that happen, and, obviously, nobody can keep a secret these days, but when people see that happen, and that becomes sort of the brush fire within the organization, that the company did the right thing, you cannot buy that anywhere. And that's a perfect scenario, but it should be the standard scenario.

Adams: And I think that's a great place to end today. I can't thank you both enough for joining us here on "The Presumption of Innocence." I think the lessons that we learn from talking through some of these variables, talking through it in a both real-world application perspective and hypothetical, from sort of the social science perspective, is really, really fascinating. I think that our listeners really can take away today a lot of things to be mindful of. And there's no one cookie cutter for this thing. I mean, this is a customizable approach and something that's really a work in progress once you get it off the ground.

And I think that's the only way you can really build towards this culture of compliance. And, if that's the goal, and that's the way that you can keep an organization functioning in a highly regulated environment, I think we've given a lot of people a lot of food for thought today.

So I can't thank you enough. Until next time, this is "The Presumption of Innocence." I'm your host, Matt Adams. We'll see you then. Take care.