FRAUD TALK – EPISODE 90

What Do Conmen and Entrepreneurs Have in Common?

There's a simple thread that connects entrepreneurs and conmen. Alexander Stein, Ph.D., discusses this connection and dissects how the psychodynamics of fraud can help fraud examiners spot the differences between ethical employees and malevolent ones. Dr. Stein will be keynoting at the 2019 *ACFE Fraud Conference Canada* in Montreal.

Transcript

Emily: Hello and welcome to this edition of Fraud Talk, the ACFE's monthly podcast. I'm Emily Primeaux, associate editor of *Fraud Magazine*, and I'm joined today by Dr. Alexander Stein. Dr. Stein is founder of Dolus Advisors and a principal in the Boswell Group and is an expert in human behavior and decision-making. Dr. Stein advises executives and boards on psychologically complex leadership, culture and ethics issues and is a preeminent specialist in the psychodynamics of fraud, corruption, white-collar misconduct, insider threats, and human factors and cybersecurity. He'll be a keynote speaker at the *ACFE Fraud Conference Canada* in Montreal, October 20 through the 23. Thank you for joining us, Dr. Stein.

Dr. Stein: My pleasure, Emily. Good to be with you.

Emily: Great. To get started, can you tell us a little bit about yourself, your background and your career?

Dr. Stein: Going all the way back, I actually began my life as a musician, which may not seem relevant to the present, but in fact, it was an early grounding in being able to listen with particular acuity to all kinds of, in essence, abstract communications. Once I made the decision to pivot away from being a performing musician, I realized that I was deeply interested in the human condition and went back to school and got a masters and a Ph.D. in psychoanalysis and trained at an institute to become a clinical psychoanalyst and began my second professional career as a clinician in private practice treating patients.

After a time, however, I made the decision to consider coming out of the consulting room to work with more impact, particularly focusing on business leaders and people in positions of influence and responsibility. I started writing a column for Fortune Small Business magazine on the psychology of entrepreneurship which was very helpful in making that transition more credible.

Then a prominent fraud litigator — actually Martin Kenny, who won the Cressey Award by the ACFE a number of years ago — reached out to me as my reputation expanded, seeking my help in working with him and other members of FraudNet to bring to bear more sophisticated psychological understanding of fraudsters and their enterprises and to assist in the recovery of stolen assets to be able to bring about a more effective conclusion to those matters for victims.

That was my initial introduction into the world of people doing bad things in essence. From there, I expanded my deliverable areas to include executive misconduct and other forms of enterprise

malfeasance, and a natural expansion to that has also been looking at people as the central elements in cybersecurity. As we progressed, there's much more that I can say about all of those areas and how they intersect and overlap, but that really is the introduction.

Emily: Great, so before we progress, what type of music did you play?

Dr. Stein: I'm a pianist and I played a lot of Bach and Beethoven and Brahms.

Emily: Great. Just had to know since that's where you got your start. To shift back to the fraud element, you are a specialist in psychodynamics of fraud. What does this mean really and specifically how can it be applied to our field of fraud fighting?

Dr. Stein: Psychodynamics essentially suggests looking at the deep psychology of how and why people behave as they do or misbehave in the way that they do. To bring to bear lenses and perspectives on what goes on inside people's minds that are vastly more complex than many of the behavioral models that prevail — essentially to take a deeper and more sophisticated approach to looking at how things happen so that certain kinds of crises events can potentially be better mitigated and then after the fact, to be able to have a more expansive toolset to help in recovery efforts and to put in place guard rails that might enable recurrence from happening.

Emily: In that vein, many white-collar criminals are pretty unassuming. This is something that I noticed when I was doing research on some of the articles that you've written. It's also something that we focus on here at the ACFE as well. They might be a trusted, longtime employee at a small business or your reliable CFO, so how do we begin to spot the differences between ethical employees and malevolent ones?

Dr. Stein: That is a question that immediately opens up into this broad vista where we're talking about what actually is the difference between ethics or ethical behavior and malevolent behavior and what are the warning flags or the different indicators that people might be able to notice? One of the reasons that that's so hard is because it's hard. Oftentimes, there really are no clear demarcations. It's not like you can actually superficially see somebody who looks different or necessarily behaves differently.

It's not just that people who commit white-collar crime may be unassuming. It's a very normal way of existing. Everyone lies, everyone evades, everyone is deceptive in lots of different ways. Oftentimes, unless we're talking about someone who is fundamentally a career criminal or deeply involved in some form of organized criminality, it's just somebody who is in a position within an enterprise. There can be any number of factors that play both internal and external to their workplace and even within their own sense of what's going on that can trigger an event or an episode.

How to make a determination in advance is pretty tricky. Whether it's trying to do some ethical or behavioral audit of an organization or bolstering internal controls or doing some form of hiring assessment, there are many subtleties and nuances that escape most forms of early-warning psychometric testing, for example. Other personality tests typically will not capture the signs that people think that they should be able to see in advance.

Emily: Moving on, you've said that you believe entrepreneurs and conmen may share formative experiences. I found that to be really interesting. What in your opinion do they have in common?

Dr. Stein: In a word, creativity? I think we can easily talk about malicious creativity and to consider what is it about the constitution of a person that he or she — although primarily we're talking about he — who will take all kinds of entrepreneurial brilliance and a hunger for innovation and use it in destructive, socially destructive or nonlegitimate ways, rather than something that adds value to society where it profits other people, shareholders or stakeholders. Where those two paths diverge becomes really meaningful.

Before they diverge, there are often a lot of similarities between creative people in the ways that they launch ventures that do something for them that's very important.

You were asking earlier about ethics and malice. For better and for worse, one of the things that happens when you start to tear away the constraints of ethical behavior is you have a broader field available to you.

Basically, there is no voice or no limit saying you shouldn't do that, or you can't do this. Essentially, you can do anything you want, and so you have a creativity unrestrained there, which is one of the reasons why we often find the good guys on their back foot, trying to figure out, "Well, how do we get ahead of people who are doing bad things?" Who would have ever thought to put a bomb in a shoe or the ways in which we're often surprised, even by the remarkable innovation of how certain things can be weaponized that we thought were just perfectly normal?

It does take a particular, almost artistic, mind to be able to look at something usual and say, "Yes, well, we can use that in a very different way, and I don't really care what happens if I do that. I'm just going to do it." This is where those two kinds of unique characters intersect. However, the results are obviously vastly different.

Emily: We need to be thinking just as — “we” being fraud fighters — we need to be thinking just as creatively when we're trying to prevent fraud by saying, "This is how a criminal could exploit this system."

Dr. Stein: Certainly, that can be harder than it seems when you just say it like that. The idea of “think like a criminal” is a fairly well-established perspective, certainly in law enforcement. For anybody who's looking to be able to prevent wrongdoing of some kind, you have to be able to think literally outside of the box because you can be sure that your opponent is not thinking within any boxes. You need every advantage that you can get.

Emily: Okay, I'm actually going to shift gears a little bit for these last couple of questions and move toward the cybercrime side. First, starting more with your analytic component. You've spoken about detecting bad actors using behavioral analytics. Can you tell us a little bit about how that works?

Dr. Stein: Right. Actually, the article that you're referencing was one in which I was cited as really a counter-voice to the use of behavioral analytics. I'm not a proponent of it, which is not to say that I'm antagonistic to it. I'm a big fan of technology and data analytics is important and has its place. My major concerns and my criticisms regarding the use of analytics is the ways in which it generally oversimplifies massively complex systems, and by those systems I mean people, not just things in which they are used.

Programming computer systems, let's say, to detect something about human behavior is much more limited than the people who are selling or buying these systems would want them to be or think they are, and so there's a false security that is in place. It's not exactly security theater, but it really is much less comprehensive than anyone would want it to be. For many of the reasons that I've already talked about

concerning the gap between understanding the complexity of human psychology and the way in which it gets rendered in a sort of compressed, behavioralistic sense in technology.

There are a whole lot of components to that, but in limited time, the one that I would isolate that is probably the most significant is intentionality. It's very, very difficult even for other people — as we were talking about regarding, let's say, hiring or looking at an impending, malicious event — to forecast really accurately to what somebody is thinking and when they're going to be doing something. Oftentimes, people don't know what somebody else is going to be doing until they're actually doing it and at that point, the old time is Latin for too late.

This is a fatal flaw with analytics, which are predicated largely on the capacity to be able to analyze all kinds of data clusters so that you can spot anomalous behavior or something like that, unless there may be something that will trigger a warning because it doesn't belong or there's some variable that is anomalous, but nonetheless, it's not able, at this point, to understand what a person is thinking about and what the internal processes that will translate even thought into action.

Emily: Yes, and to expand on this a little bit more and please correct me if I'm wrong, but are you basically saying that with these analytics, we fall into a trap of maybe putting a system in place and relying on that system to catch something. However, that system isn't living within our minds and doesn't know that a bad actor is considering doing something?

Dr. Stein: That's exactly correct. What you just said is not limited to technological systems. What you just stated really is a perfect summary of many of the flaws where deficiency is probably a better word in most fraud mitigation practices. There's a notion that there are certain things that you should be able to see or know or do, and if they're constructed and executed on perfectly, that it will create an airtight system or a bulletproof system that will prevent something and that's just not the case. It sounds as if I'm being extremely pessimistic in everything that I'm talking about here like, "Well, you can't do this and you can't do that."

It's not my intent to be quite so negative, but rather to shine a bright light on how much harder this all is, than people would like to think and that by and large, my recommendation as an overlay to everything is that any organizational system, if it's truly serious about looking to mitigate threat actors of various kinds, has to have a system that's designed to account for the realities of human behavior, and really have redundancies, and shock absorbers for that built into it, rather than to architect threat mitigation or defense systems that sound wonderful, but really would only work if people cooperated perfectly with them, and that's just not what's going to happen.

Emily: I feel this leads in nicely to…we're one of those organizations, those associations, that's looking to stamp this out. Here at the ACFE, we teach about prevention being a much more successful and more cost-effective tool than detection in the fight against fraud. In your experience and opinion, how can fraud examiners more successfully spot insider threats to their organizations before fraud becomes expensive and detrimental to the company?

Dr. Stein: Well, if I can continue along the path of being really darkly pessimistic here, I don't think that trying to stamp it out is going to succeed. Fraud is a part of human interaction. I think that if we were to ever find a way in a sense to inoculate against it or to eradicate the impulses that give rise to it, what we would be left with is not really something that we would be happy with ultimately. We have other choices besides complete gratification, and it involves what you're asking for, is just how can we treat this more effectively?

One of the ways is actually to take a more realistic stock of who people are, and not every ACFE member necessarily needs to have deep and extensive training and expertise in psychology, but it certainly would be recommended, I think, to advance what you're asking about, which is how can all fraud fighters of various types do better at helping to prevent these kinds of things from happening. When they're deployed into an organization, to be able to know and think about things that are really outside their professional domains and not to minimize or dismiss them because they don't understand it or because they don't think it's relevant or because they don't think it's really important.

There is nothing that's unimportant in the ways that people think and behave. Often, it's the minutest, seemingly innocuous detail that actually becomes the critical thing. Helping people at least to raise not just their awareness but their potential and their capacity to take notice of things that don't relate to, let's say, spreadsheets or transaction details or other hard commercial elements of something that could be evidence of criminality or some form of wrongdoing. Really to be able to pay very, very close attention to the nuanced human dimension will go a very long way.

Emily: Okay. Great. Just to finish this off, is there anything that you would like to cover that I may not have asked, maybe something in the cyber realm before we go?

Dr. Stein: I appreciate your asking. I think I actually made the strongest point just then that I can and that relates not just to members of the ACFE and other fraud-fighting professionals but really people in positions of influence and responsibility in decision-making at the tops of their organizations or the divisions and business lines that they had as well as other affiliated professions who are engaged in doing what they can, whether it's in information security or compliance and ethics or capital management to learn more and be more attentive to the complexities of who people are and what goes on with people in organizations.

Now, one of the worst things that we can do and actually one of the ways in which we all end up enabling wrongdoing is by oversimplifying and pushing things to the periphery, and suggesting, "Well, it can happen here," or "We've done everything we need to," or "This really isn't important." All of the different ways that we have and that people use every day for minimizing or avoiding lots of things that are very, very challenging.

Emily: Well, great. Thank you so much for speaking with me today Dr. Stein.

Dr. Stein: My pleasure, Emily. Thank you for having me.

Emily: Remember you can find more episodes of Fraud Talk at ACFE.com/podcast, the iTunes store or wherever you get your podcasts. This is Emily Primeaux, signing off.