



# **Best Practices in Preventing Fraud and Corruption in Global Business With Attention to FCPA**

## **Best Practices in Preventing Fraud and Corruption in Global Business With Attention to FCPA**

ROBERTO SCALESE: Good morning. The Association of Corporate Counsel and SmartPros Legal and Ethics welcome you to today's webcast, "Best Practices in Preventing Fraud and Corruption in Global Business With Attention to FCPA [Foreign Corrupt Practices Act]."

*[The instructions provided here were intended for attendees of the live webcast when it was originally broadcast. You may submit questions and comments regarding the content of this course using the [Questions and Comments](#) link on the left side of your screen below the video.]*

Our presentation today will be moderated by Alexandra Wrage, president of TRACE International. Alexandra will introduce today's speakers. Take it away, Alexandra.

ALEXANDRA WRAGE: Thank you, Roberto. Before I begin the introductions of our sponsor and panelists today, I'd like to ask Roberto to launch a quick poll question to assess audience familiarity with the Foreign Corrupt Practices Act. So, Roberto, if you could launch that, and if everybody would take a moment to respond.

And while you do that, I would like to thank on behalf of the Association of Corporate Counsel, the sponsor for today's event, which is Lex Mundi. We'd like to thank Lex Mundi and its business crime and compliance practice group for their kind sponsorship of this webcast. Lex Mundi has a long-standing relationship with the ACC and has provided legal expertise to ACC members worldwide for many years. They have 160 law firms in over 100 countries, designating one top-tier law firm per jurisdiction. Please look for Lex Mundi at the ACC annual meeting next month in Boston.

I am joined today by three panelists, all with a high level of expertise in this important issue. We're going to hear from Wally Dietz, Frank Eichler, and Ross Booher. Wally Dietz is a graduate of Georgetown Law Center, after which he served as a legislative assistant to U.S. Senator Jim Sasser when the FCPA was first enacted. He has practiced at Bass, Berry & Sims since 1983 and is co-chair of the firm's internal investigations and special projects practice group. He has extensive experience with investigations involving the FCPA, the False Claims Act, the SEC [Securities and Exchange Commission] regulatory issues, and has acted as a counsel for a monitor appointed by the SEC to assess compliance with a nationwide remedial order.

We're also going to hear from Frank Eichler, who is chief administrative officer and general counsel for Ozburn-Hessey Logistics [OHL], a leading provider of global supply chain management solutions. OHL has more than 120 distribution centers on six continents. Prior to joining OHL, Frank served as senior vice president and general counsel for Dex Media, which he helped to take public, and prior to that he was general counsel to Media One Group.

Finally, we'll hear from Ross Booher, who is a partner at Bass, Berry & Sims. Ross concentrates on complex litigation, internal investigations, and FCPA compliance. He was previously a prosecuting attorney in the U.S. Navy's Judge Advocate General's Corps, serving in Asia, the Middle East and Europe. Ross' experience includes criminal and national security investigations in foreign jurisdictions.

Before we launch into the substance of the topic, I wonder, Roberto, if you could just give us a quick summary of the poll results?

ROBERTO SCALESE: Thank you, Alexandra. I have the poll results. The respondents—54 percent said yes, they do have prior experience with the FCPA.

*[The CLE code and instructions provided here were for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast when you have finished listening to it, click the EXIT COURSE button at the top right of the screen to return to your My Courses page and then click the certificate link or icon beneath the course listing. In the pop-up window, select the desired jurisdiction from the drop-down list and enter any requested data, such as your bar number and the CLE code that popped up while you were playing the archived webcast. (This code is required for New York and Ohio attorneys only.)]*

ALEXANDRA WRAGE: Great, thanks so much.

So, the FCPA [is] a highly relevant topic—a topic that has been in the news a great deal lately, with staggering sums and widespread consequences for corporations internationally. There is an overarching theme in the FCPA world right now, which is just more: more prosecutions, more and larger fines, more prison sentences for individuals, more and greater jurisdictional reach, more industry-wide investigations, where the Department of Justice [DOJ] starts with one company and then has the investigation spread to other companies in the same industry. And outside the U.S., more countries [are] prosecuting under their own antibribery laws. The FBI has set up a dedicated FCPA team and now the SEC has announced that they intend to follow suit.

The U.S. has assessed \$1.3 billion in fines and disgorgement in the last 10 months alone, and the most prominent among the cases that we've been hearing about recently was the Siemens settlement, which itself, between the United States and Germany, was assessed \$1.6 billion. But in that case, as in so many cases, the fines themselves are often considered the smaller part of the penalty, because the remediation efforts and [other] expenses associated with these can mount much faster than the fines.

So, with that, I would like to turn this over to Wally, who is going to walk us through the basics of the FCPA. We have about half the people on this call who are fairly new to the topic. We'll move through this quickly, but over to you, Wally.

WALLY DIETZ: Thank you, Alexandra. I'll go forward now with just a very quick discussion of what is the FCPA. This statute was passed in 1977 in the wake of the Watergate scandal and the Church Committee investigations of activities of the U.S. abroad. It's been amended a couple of times since it was initially enacted.

One thing we'll be talking about during the course of the seminar this morning is that we have parallel enforcement. The DOJ is involved in enforcing the statute, and the SEC is also involved in enforcing the statute.

Let's look at first the antibribery provision of the FCPA. The FCPA importantly has two main components. One is the antibribery provision. The other is what's called the "books and records" provision. We'll talk about both of those briefly.

You can see on the slide [that] the antibribery statute prohibits corruptly offering or providing anything of value to a foreign official for the purpose of influencing the official to do anything that assists the offerer in obtaining or retaining business. And I walked through that slide because, as you can see, for us lawyers it opens a can of worms of questions: What does it mean to offer anything of value? Who is a foreign official? And then you get to the intent, for the purpose of influencing the official to do anything that assists the offerer in obtaining or retaining any business.

So, there are some vagaries built into the statute that we will talk about in greater detail. Things are not so clear-cut. You may be thinking about a novel or movie script where "corrupt" sounds like suitcases full of cash, and, in fact, it's a lot more difficult to analyze than that.

Also, notice there is no success requirement. All that is required is that the payment or offer be made with the requisite intent.

Now, going to the next main component of the FCPA, which is the books and records provision, it requires that issuers—and that’s a defined term—must keep books and records and accounts which, in reasonable detail, accurately and fairly reflect the transactions, and it also requires that issuers maintain a system of internal controls. And this becomes a main focus for both the SEC on the civil side, but also the DOJ on the criminal side. This statute imposes affirmative duties on issuers.

And I might ask Frank, since he is in-house at this point right now, Frank, do you see a difference between this standard and what’s required under Sarbanes-Oxley [SOX]?

FRANK EICHLER: Not really, and I think you have to be careful, because Sarbanes-Oxley gives a false sense of security in that you can have your auditors or your company say, “Well, you’ve got accurate books and records,” but if you’ve got a small office, like we’ve got one in Thailand that’s only got like 20 people in it, it doesn’t rise to the level of materiality that our auditors would look at it. But I still have to comply with the “no materiality” and the FCPA in that office, even though it might not rise to the SOX materiality, so you have to be very careful there.

WALLY DIETZ: OK, so as we can see, there is a difference, whereas you have a materiality standard in Sarbanes-Oxley, there is not one in this statute.

Also, moving quickly to the jurisdictional reach of the statute; it’s very, very broad. We’ve shown you on the slide the definition of “domestic concerns,” which is a very broad definition. It applies to corporations [and] partnerships. Importantly, as we’ll talk about in great detail, it very much applies to individuals, who have liability under this statute.

And the definition of an entity: We’ve seen in our experience that some clients, for instance, who were nonprofits—such as universities or charities—they may feel like it doesn’t really apply to them, but in fact, it does, and we’ll talk later on about how even Alexandra’s organization has used the DOJ opinion release procedure to ensure compliance. So, the jurisdictional reach is very broad. U.S. and foreign entities and individuals have been prosecuted under the statute, and, frankly, many individuals, including your clients, may not even realize that their conduct is subject to the governance procedures of the FCPA.

Now, we’ll talk a minute just about the breadth of the statute. For instance, as we discussed, we’re not talking about suitcases full of hundred-dollar bills being given to heads of government. The definition of who is a foreign official is, in fact, a very complicated matter. In some countries, in some jurisdictions—for instance, if you were in the health care business, almost everyone in the health care business would be deemed to be a foreign official. For instance, a physician in certain countries, if it is a state-run health care program, could be deemed to be—and probably would be deemed—as a foreign official. It applies to political party representatives and officials. It applies to employees of public international organizations. We’ll talk again about how this is a broad definition.

Also anything of value, [as] we’ll talk about, could be deemed to be excessive travel—first-class as opposed to coach—gifts, jobs for relatives, anything of value. We’ve got a slide of a castle up here on the screen, and the reason for that is—that’s known as Chudow Castle—and there was a case with Schering Plough where they made a donation to a charity to renovate this castle in Poland, but they described it on their books and records as health education, and they ended up paying a half-million-dollar fine to the SEC for the enforcement action because, in terms of the books and records requirement, they did not accurately describe that. So, “anything of value” is much broader than cash in a suitcase.

There is also liability for the actions of third parties, if we could move to the next slide quickly. If you are involved or

your clients are involved in operations in foreign jurisdictions, it's very common to use agents, and these agents are very often your biggest risk. And it is inappropriate in this day and age of enforcement activity to put your head in the sand about who your agent is, who their relationships are with, what conduct they are doing, and the actions of the agents can be attributed back to the company and can get you very much in hot water with the government.

Now, let's talk quickly about what happens if there is an FCPA violation. We've got a slide up showing corporate liability, which includes everything from felony convictions to very large fines to disgorgement of ill-gotten gain. If you are in the health care business, for instance, you can be debarred from doing government business. If you're in the government contracting business, you can be debarred from doing government business. The government can insist on a compliance monitor, which is very intrusive and expensive. Also, you have very large defense costs. Siemens alone paid out over \$800 million just for defense costs. Also you have the risk of other types of lawsuits being brought if there is an FCPA violation—a derivative claim or a class action [or] other sorts of litigation.

In the course of this presentation you are not likely to hear us talking about corporations taking a lot of these cases to trial because the risks are too high. And obviously, if you are a public company, the impact on a public company of an FCPA violation and investigation can result in very adverse material impact on your stock price, and we've just shown you a couple of examples of that briefly. That pretty much goes without saying.

Turning now to individual liability: Again, there is the risk for individuals who are liable under the statute to be convicted and go to jail and, in fact, that is happening as we speak. [There is] imprisonment of up to five years per violation. There are fines—both civil and criminal fines—and there can also be a requirement that ill-gotten gain be disgorged, and individuals can be barred from government contracting opportunities, and obviously it's a reputational issue. And in terms of your officers and directors, for all of the in-house counsel here, as you know, with any indemnification issue, if an individual is in fact liable and culpable for this conduct, there can be no indemnification by the company.

So, some of you may be wondering: With all of these issues, what can you do? There are a couple of affirmative defenses. One is reasonable and bona fide business expenses. You can pay those to foreign officials, if they are both reasonable and for a bona fide business purpose, and if they are lawful under the local law. Now, there is also an exception under the FCPA for facilitating payments, which are the kind of payments made to expedite or to secure the performance of what is viewed as a routine government function such as a nondiscretionary permit, such as getting a utility permit—getting your lights turned on. And it's sort of to grease the tracks. And it's permitted under the statute, although increasingly it's highly disfavored by companies in terms of opening the door to other requests for such payments. Also, if the payments are too large they, by definition, cannot be viewed as facilitating payments.

ALEXANDRA WRAGE: Let me jump in there for just a second and ask Frank, as our representative of the in-house community, his position on facilitating payments and how he perceives them.

FRANK EICHLER: Thanks, Alexandra. To be honest with you, it sounds very easy, but it's very difficult to clearly fit within the four corners. I have always counseled to avoid [them]—way too much risk—and one thing we have to remember is: Anybody coming in and looking is always going to look with hindsight, and most of the time they're not going to claim that the facilitating payment really is that. So, I'd avoid it.

WALLY DIETZ: And again, in terms of what can you do, we can go to the next slide. If we're talking about legitimate business expense, the main takeaway here is that there is a disconnect oftentimes between our clients, who have certain lifestyle expectations, and what a government regulator may view as reasonable. For instance, clients are used to first-class travel sometimes—or even company planes or whatever—and the government investigator is likely not to view that as a reasonable expense. What sort of hotel you choose for accommodations could also be challenged, and think about, when you're making these decisions: The lifestyle of a government investigator or government attorney versus the CEO or CFO [chief financial officer] of your company. There is just very much a difference.

We had a mediation with the DOJ a couple of months ago, and the lawyer came in, he took one cup of coffee, and when he left our office, he paid our receptionist a dollar, because he didn't want to be viewed as being given anything of value. And that tells you just a little bit about that mentality. So, I'll pass it now to Ross, who is going to take us through a road map of the statute.

ROSS BOOHER: Great, thank you, Wally. So, we're going to start out here: Why is the FCPA relevant now and what are the trends to watch?

Well, first of all, this is a major political priority. [There are] a few headlines up here for you to give an example of what we're talking about. There [are] significantly increased resources right now being applied to FCPA enforcement in the United States. There's a dedicated group at the Department of Justice in D.C. of attorneys who do nothing but FCPA work. There is a dedicated FBI unit that is assigned to do nothing but FCPA investigations, and, as of quite recently—as of August 5 [2009] —the director of enforcement at the SEC, Robert Khuzami, has announced the creation of a specialized FCPA unit that will be pursuing even more aggressively FCPA enforcement at the SEC.

Now, to put some context around this, why is this happening? First of all, obviously the statute has been around for quite a long time, but for many, many years, the U.S. was one of the only countries that had this type of law in place, and there is a widespread perception that it just disadvantaged U.S. business; that there was unfair restrictions on U.S. businesses, whereas other companies could pay these types of fees, could engage in this type of conduct, [and] could essentially pay to buy influence.

As a result, there was political reluctance to aggressively enforce this law. In fact, in some other countries, companies could actually take tax deductions for payments to obtain or retain business from foreign governments or government-run business officials. So, that has significantly changed, due to the implementation of the OECD [Organization for Economic Cooperation and Development] antibribery convention in the late '90s, which now has approximately 38 signatories, and the implementation of similar laws in a number of other countries. There is now enforcement not only in the U.S., but worldwide. As a result, the U.S. political will to enforce has increased dramatically.

And so, what we see is broad international enforcement increasing; just a couple of the examples that are up there. Obviously the most stark example of international enforcement cooperation was the Siemens action, which was announced simultaneously both in the U.S. and Germany on December 15 of last year [2008]. And so, right now, if your company is encountering an FCPA problem, it is very likely that you'll have a problem not only with the U.S. government, but also with the government in which the problem occurred.

Just to give you a quick rundown of what all this means and how we can see the effect of this increased political will and increased resourcing of FCPA enforcement. Here's just a quick snapshot of some of the recent enforcement actions, walking back to December 15 [2008] and going forward to just a few weeks ago. And again, it's important to note that these figures only reflect U.S. enforcement, not the enforcement in other jurisdictions that is also oftentimes occurring.

Also, note that this is not just massive companies. Obviously, there's some huge ones there—Siemens [and] KBR, for example—but there are a number of smaller companies that are also facing liability. In 2008, for example, AGA Medical, a medical device company, agreed to a \$2 million criminal penalty as a result of payments that were made over an eight-year period in China. Now what was interesting about that is: The company was relatively small, and over that eight-year period, their revenues from overseas operations totaled only approximately \$13.5 million. Their overall annual revenue for the company, in 2007, was only approximately \$150 million. So, here's an example of a company with very little overseas involvement but with a very, very big FCPA problem. So, just because your company doesn't have a great deal of overseas involvement does not mean that it can't encounter enormous liability.

Now, again, as Alexandra mentioned in our opening, individual enforcement has dramatically risen. This is just a quick snapshot of some of the recent enforcement actions against individuals. And as you can see, it's extremely small; we've only included some of them, and they're just happening on a literally one after the other, both from the DOJ perspective and SEC enforcement actions. It's a major trend. We're talking about significant prison exposure, huge fines, and, for foreign individuals, the U.S. is actively seeking to extradite foreign nationals from other countries. And so, this individual liability is beyond just the United States.

Two quick snapshots, in terms of the examples of individual liability: In the Nature's Sunshine case, you see there's a reference up there to two executives. This is unique. This just occurred a few months ago, and what's significant about it is that these two executives ultimately paid a civil penalty and it was based on control person liability. The SEC, in its enforcement action, did not allege that they had personal knowledge of what was going on. Instead, these individuals were sanctioned and ended up settling because they were held responsible for having failed to put in place sufficient internal controls and compliance efforts. So, it's not just the person who's actually involved in the transaction, it's exposure for people who are corporate executives who should be putting in place compliance. And that is something very important for company executives to recognize.

A number of other examples: The Diaz case; the Diaz reference there. This is another good example because it shows how sometimes this liability can arise. Perez, who's reference was controller of a telecom company. He approved payments to a vendor, which was run by Mr. Diaz, and these were consulting payments to the vendor, but in fact the vendor was not providing any real services, and instead they were being used to gain influence with a telecommunication company (a state-owned entity in Haiti). So, the use of third-party agents and vendors [is a] major, major exposure.

In the last year—actually in the last eight or nine months—there have been three criminal trials under the Foreign Corrupt Practices Act. This is remarkable, and it signals the dramatic increase in DOJ criminal prosecutions of individuals, and that's something that we can probably expect to see. And one of the reasons you see these going to trial is because of the massive exposure and the long prison time that individuals have a huge incentive to fight.

Sources of investigations: How would a company likely come to the attention of an enforcer? First and foremost, whistle-blowers [and] disgruntled employees. The more headlines that appear in places like *The Wall Street Journal* and *The New York Times*, *The Washington Post*, etc., the more people realize just how broad the requirements of the act are. And many times people see those and they realize that there is conduct occurring within their own companies that is inconsistent with these legal requirements. And they either call in—sometimes they try in their own company and don't get anywhere—and then they call the FBI, the DOJ, the SEC. They call the Serious Fraud Office in the United Kingdom and those allegations are transmitted back to U.S. enforcers. This is a real issue post-Madoff. You see that the SEC and the DOJ—the SEC in particular, obviously—are very sensitive to following up on allegations.

Competitors: You know you're in a competition with foreign firms, you win, and everyone else thinks the only way you won is because the fix was in and there was some improper influence. They make the allegation, and now you're facing a situation where your company needs to be able to demonstrate that there was no improper activity occurring.

Customers: Customers sometimes can be subject to an inquiry, and in the course of being asked questions about their conduct, they're asked questions about everyone they deal with. And that is a way you see some of these investigations spider-webbing out from a customer back up their supply chain.

Foreign enforcers: Again, [if] you have a problem in a foreign country, they're likely to pick up the phone and call U. S. authorities.

And last, but certainly not least, is the subject of active investigations. We have heard directly from members of the FBI's FCPA unit that they are using all the resources available to them to investigate these matters: wiretapping, covert

resources, just the types of things that they already have available to them [in] some of their other sections and departments—available to them to look into things in foreign countries. So, it's important to realize how serious the investigative potential is.

So, what are the trends? Alexandra hit these briefly at the beginning of our presentation, but just quickly, first and foremost, [there's] increased individual exposure. The DOJ has made it crystal clear—as has the SEC—that they want to hold individuals personally responsible, and they know that's the best way to get people's attention, and that is exactly what is happening. This means more jail time and it means a lot more focus on individuals.

This is important for a couple of reasons, one of which is because once the focus rests on an individual, that person is going to be concerned about spending a long time in jail, and they are likely to want to be cooperative with the government and tell as much as they can about everyone else in the organization and everything else, and not just FCPA issues, but any other thing that they can use as a bargaining chip. And so, that is a huge enforcement tool and why compliance in this area and every other area is so critical when you're dealing with international business.

Second: Increased risk of corporate exposure. We've heard directly, again, from DOJ; they are referring to this as the "era of big risk." If you are doing business overseas, then you are undertaking big risk, because if you have an FCPA problem, the consequences are so devastating.

We talked about the increase risk of foreign enforcement. Increased scrutiny of private commercial activity is also important. We've seen the DOJ get involved in investigations and perhaps determine that there is no foreign official involved. The entity that may have at first appeared to be state-owned is, in fact, purely private. And instead what you see occurring is: They then determine [whether] there any applicable commercial bribery statutes that can be applied—perhaps incorporated through the Travel Act, for example—and they will pursue a prosecution from that angle once they've invested a lot of enforcement resources. So, that's important to note. And again, increased risk of foreign prosecutions. Many of you have seen the recent arrest of individuals associated with the large company Rio Tinto in China, and there's just significant risk there.

As an example, our Lex Mundi member firm in Germany, the Nörr firm, recently advised us that the German Supreme Court has recently released a decision in which the court has found that fraud can be committed by omission by a compliance officer. And so this is very significant, because it effectively means that a compliance officer, under some circumstances, is viewed as a guarantor, and if they fail to prevent corruption, according to the assessment of the Nörr firm, then you are at risk of being prosecuted criminally for that. So, it's important to understand what are the anti-corruption laws in each of the jurisdictions in which you operate, not just in the United States with respect to the FCPA.

And then, of course, this all adds up to incredibly high expectations for corporate compliance. Wally and Frank, I'll just throw this out to you. First of all, Wally, what are your perspectives in terms of this trend, what you've seen in your work?

WALLY DIETZ: Well, I think the only thing I would have to say is that we've had conversations recently with both the DOJ and senior enforcement officials in the Enforcement Division of the SEC, and their message was alarmingly the same. They both have used the words "era of the big risk," and said if you were not advising your clients that they are in an era of big risk, you are not doing them a service.

ROSS BOOHER: And Alexandra, let me ask you. You recently have been with Secretary of State Clinton in Africa and President Obama in Russia, when they've been addressing these issues of foreign corruption. Based on your experiences—those and others—can you give us your perspective on these trends?

ALEXANDRA WRAGE: Yes, absolutely. I think the trends are set to continue. I think there's just no disputing that at all. Not only has President Obama included references to corruption in his Moscow speech and again [elsewhere], but the whole administration—Secretary of State Clinton, as you mentioned—and eight of her stops on her Africa [trip] mentioned the problem of corruption and connected it to foreign direct investments during the GOA [African Growth and Opportunity Act] forum in Nairobi. We've also heard comments from Eric Holder of the Department of Justice, and Mary Schapiro with the SEC, so everyone is making it very clear that this is going to remain a topic.

The other side of that is the number of cases that we see coming out this year are pretty direct in the pipeline, and the DOJ delights in affirming for all of us that there are more cases in the pipeline right now than there ever have been before, certainly more than 100. So, both what the administration is saying and what we see the Department of Justice doing [should] prepare us for another wave.

FRANK EICHLER: Ross, if I can jump in [for] a minute. Also, at least from the business standpoint, I'll tell you that the compliance expectations are a lot higher than they were a couple of years ago. So, those of you who are general counsel for companies, if you've acquired a company, if you've got a new agency agreement, a different subcontractor, if you haven't updated and re-examined your compliance program in the last couple of years, you need to do it now. It is a whole new environment and I think it's just one of those things that not only needs to be refreshed, but you really need to dig into how you do it, where you do it, and the depth you need to go, and where you're doing business in.

ROSS BOOHER: Great. With that, I think we're going to move onto the next step, and I'll throw it back to you, Alexandra.

ALEXANDRA WRAGE: Yes, thank you. I guess I'd like to pick up on what Frank just said and see if we can't drill down on that a little bit and find out, with this current enforcement climate and assessing risk as you indicate, what are some of the factors that in-house and outside counsel should be considering when they're evaluating that specific client's FCPA risk?

FRANK EICHLER: Sure, and go to the next slide please, Ross. The biggest one is where you do business. And we'll talk about that in a minute (you'll see a slide). But the jurisdictions where you do business, how many touch points and the types of touch points you have with foreign officials, and again, sometimes these foreign officials can be ones that you don't even know are foreign officials. We had a company that we were doing business with in China that had some customs people, but we didn't know that those customs people internal to that business were actually customs officials and therefore fell under the FCPA, so you need to be real careful there.

Also, certain industries have heightened scrutiny. Your energy infrastructure, your telecom, health care and transportation are all key focuses.

The other thing is: It's how you're using the foreign subsidiaries, your joint ventures [and] third-party agents. I really want to emphasize that agent risk. It is amazing to me how many agents we use in our business, and we have to make sure that they're all complying and they're doing what we [want], because basically it falls to us, so be very careful about that.

The next slide, basically—and this came up not too long ago. We were making a couple of acquisitions, and I went to this slide and found out that all the acquisitions we made were all in the red territory, so it caused me a little bit of a concern. The redder the country, the higher the risk, and I think you need to base—again, make sure that you [know] where your employees [are] and where your agents are, where they're visiting, where their operations are. It just is crucial. And like I said, where the red is, that's where you've got the highest level [of risk]. You need to be very careful about that. And if you haven't done an updated comprehensive compliance program in those red areas, then there's a high likelihood that you will not meet some of the standards for the DOJ, and they're going to have a lot less

sympathy if you haven't done a regular program in the areas that everybody knows are high-concern areas. You're just going to be kind of walking yourself into a problem.

The other thing is: I think we've got some red-flag areas here. And you can read these. Other than these, one of the things I've always looked at: We had a couple [of] stations or offices in certain countries that always made the same amount of profit every year. And after about the second or third year, you wonder why, and then, when you go in and look at that office—and again, it was a small office; it wasn't material—but you really need to take a look and say, “OK, what's happening here?” And we did have some issues there so we had to clean them up. So again, be aware of the red areas, be aware of the red flags, and put together a well-thought-out program, and I think you'll be able to address some of the issues.

ALEXANDRA WRAGE: OK, that's great. I wonder, Ross, if you'd like to expand on that a little bit. There are certain tasks that are very appropriate to in-house counsel and how they handle this risk, and particularly identifying the risk early on. One of the questions that's come in is: “We have operations in—I won't name the country, but in a country that's considered reasonably high risk—and I have suspicions that there might be inappropriate payments. No proof whatsoever, but suspicions. What are some of my obligations?” So, maybe that's a question that an in-house counsel would lob to outside counsel.

ROSS BOOHER: That's an excellent question. That's one that is very, very common. So let's just walk through what a framework would be for addressing this type of situation, whether you've gotten a specific red flag or concern or report, or you're sitting there and you think, “I've never heard anyone express any concerns about this at all to me.” This would be a framework to consider.

First of all, you want to assess your risk. As Frank described: jurisdictional; what are your touch points with the government? Where do we do business? Just because we don't consider ourselves an international business doesn't mean that you're not. Do you buy things from overseas? Do you sell things overseas? Do any of your employees travel overseas? Et cetera. Second, establish a compliance program to reduce your exposure, and third we're going to touch on acquisition due diligence. So, let's get into this just in a little more detail.

First of all, again, assessing the risk—how would you do this? The first step is to make sure your key compliance employees know the requirements of the FCPA. It is not uncommon at all for us to go into very large, sophisticated corporate entities—whether public or private—with in-house legal departments, and find there to be very little knowledge of the broad—both prohibitive and affirmative—responsibilities [and] duties under the FCPA. So, the first thing you want to do is brief all your key compliance employees and make sure they understand it. Second, you're going to identify your risk areas. Third, you want to review your code of conduct and your current FCPA policies and procedures and make sure that they are up to speed and consistent with the guidance that can be obtained from the current SEC and DOJ actions.

The next thing you're going to make sure that you do is: You need to review all of your third-party and agent contracts, where they have any implication at all for conduct outside the United States. Do they have [representations] and warranties in them? Termination clauses? Have you done a thorough process of making sure the people you're retaining are—there's been sufficient due diligence, you haven't ended up retaining someone who is going to cause you a major problem, and that you have a system in place to assess their compliance, to make sure that they're not going to run your ship into the ground, because they are going to be considered to be acting on your behalf.

And then, number five, you're going to want to thoroughly review your accounting [and] internal control processes. Again, as Frank mentioned, just because you have a SOX compliance program in place, there is no materiality standard for the FCPA, and so you're going to want to make sure that the level of detail and review is going down to a very, very fine, granular level.

So, let's talk quickly about what we've called the DOJ talking points. If you were to ask an enforcer, "What are we going to be looking for?" If your company has a problem and the DOJ comes calling, or the SEC comes calling, this is what the DOJ and the SEC are going to be looking for, and this is what they're expecting.

And first of all, let me just stop here and say: You may be thinking, [with the] tough economic times, "Is there any appreciation for how much my time and how much my executives' and business people's time will be taken hitting these points?" That question has been posed directly to enforcers. I've heard it in a number of situations, and the answer I've heard enforcers say is, "If you can't afford a compliance program and to take these steps, then your company cannot afford to do business overseas, period." So, just be aware that that is the perspective of enforcers.

So first of all, tone at the top: This means that it's got to be clear that your senior executives have bought in to compliance and this really matters. Not just the compliance officer, not just the GC [general counsel], but your CEO, your [executive vice president] of sales; it's got to come down all the way. And one of the ways you can make this clear is: They're going to be potentially criminally liable, and so that can be conveyed to their subordinates, that, "Hey, your conduct affects me, and that's why I expect you on my team to keep us within the lines completely."

Number two, corporate policy delivered from the top to all relevant persons. Again, [with] your policies and your procedures, people need to understand that if they get outside the lines of those policies and procedures, it's not just something the compliance person is going to care about, that it's going to be something the CEO is going to be concerned about. And so, just to touch on that, I guess, Alexandra or Frank, in terms of the types of policies, in terms of making sure that they are geared towards their audiences and so forth, can you all jump in and touch on what you all have seen as effective approaches to developing policies and procedures.

ALEXANDRA WRAGE: Sure, absolutely, and you hit on some of the highlights. The management message is incredibly important. And you talked about how expensive this can be, and that's worth noting, but there's also some very cost-effective solutions that can get maximum exposure for a new program without a lot of expense. Even a rollout initial e-mail from the CEO to everybody in the company talking about the importance of this issue, really putting some weight behind it and indicating seriousness of purpose. And that seriousness of purpose may be manifest in allocating budget, in allocating the appropriate number of people to the process, making it all very accessible: Not only the document, whether it's online or hard copy—although I suspect most are online now—but the language, making sure it's not dense legally, making sure it's translated into all appropriate languages, so that the people who need it out in the field can have access to it quickly.

We talked about updating policies a little bit earlier, and I think that's critically important. If you're rolling out new products in new markets, with potentially government customers where perhaps you didn't have them before, you'd better be updating your policy at intervals to make sure it's still applicable to your current business model, including acquisitions and entering new markets.

And two other points, just very quickly. One is making sure that your employees have somewhere to go with questions that is not necessarily in their reporting chain. A lot of this stuff is very difficult. The lavish gifts you talked about, charitable contributions; it isn't always intuitive. I mean, I'm sure that everybody on this line has a pretty good sense that cash for business has been criminalized now, certainly in the U.S. and in most countries elsewhere. But [with] the subtle issues around travel for government officials, and that sort of thing, people often need advice on those. And they want to get advice from somebody who isn't necessarily managing them directly, so making that available, either through a hotline or a help line or some other system.

And then the other thing, and nobody ever likes to talk about this, is sanctions. If you have this fabulous, shiny, new compliance program and you've rolled it out effectively and everybody has read it, and then people start violating it and there are no consequences for that, then you really have gutted your program at the outset, because it's really perceived from the outside as a paper policy and not more than that. I'm sure Frank's experiences, though, will enable

him to add to this list considerably.

FRANK EICHLER: You hit almost everything, Alexandra. Keep it simple. Local language is important, and we've always used examples tied to the local situation. So, for instance, we've got great access here to the Lex Mundi legal network. Talking to that group of lawyers, having them identify kind of what's happening in their country—use examples, maybe even having them come to the main meeting—it is amazing how much impact that has. Because again, when I walk in to a different country, they have no idea who I am. But they do recognize local people and speaking the dialect and everything else. It works very, very well.

ROSS BOOHER: Great, well that is—just to emphasize that point. If you're, for instance, doing business in India or, let's say, South Africa, you may think that your company is safe so long as you're complying with the FCPA. Let's use the South Africa example. Their laws, in some aspects—anticorruption laws—are even more strict than in the United States. So if you haven't plugged in with a local counsel there to make sure that you have layered into your compliance program for your work in that country their local requirements, you have left yourself a gap that can result in criminal liability in that jurisdiction.

So, just quickly, again, we've hit tone at the top [and] corporate policy. This third item [is] senior compliance chief who reports directly to the audit committee. And let's see, training of directors, officers, employees and agents: Again, we've touched on that. Appropriate disciplinary process. Reporting system with an anonymous hotline—again, as Alexandra said, this is critical. You want to make sure that [with] these reports, there's an ability for someone to be able to get a report to the compliance officer, to the GC [or] to the audit committee in a way that their job is not in jeopardy. And you also want bypass procedures so if they're making an allegation against a senior official of the company—say the general counsel or compliance officer—that it automatically bypasses them and goes to a board of directors member, so that employees can have confidence that their reports are getting through.

And just to make it clear, there are systems out there—there are a number of vendors out there—that you can use and you can maintain contact with the person making the report. They log on to a computer screen, it gives them a number, they make their report, and they can log back in to that screen using their number, and they don't have to ever give their name or any other information. That enables the company to be able to communicate back and say, “All right, thank you. Can we get more information?” And that can save a company an enormous amount of money in terms of internal investigation resources, if you can maintain that communication while also maintaining confidentiality.

FRANK EICHLER: Ross, can I jump in here a second? In today's world of using the Web and everything else, Internet-based training is great, but I'll tell you [what] you really need to have. If it's a brand new company, I stress the importance of the in-person [training]. It creates more question and answer, and you can always tie it in with a regular meeting you're going to make to that country or that station. It really is important. Don't do everything by the Web and just expect everything to happen perfectly, and they just sign up and it's done.

ROSS BOOHER: I completely agree. Quickly, on due diligence and acquisitions, Frank's going to touch on that a bit more in a moment. Periodic audits: Again, you need to be swinging through your operations overseas and having people on the ground checking on these things [and] interviewing people. Because again, if you don't actually have someone periodically speaking with people, you're not going to ever see a lot of problems that could be there, because in a lot of cultures they're just not going to engage electronically or by phone, or talking to someone that they do not know and have not seen. And as Frank earlier mentioned, [take a] tough look when you're in those red flag areas.

Obviously, there [are] a number of benefits to compliance beyond just keeping executives and employees out of prison and avoiding the total fines, and so forth. Having a good compliance program also makes you a better candidate for gaining government contracts, detecting other problems within the company—waste, fraud, abuse. And if your company's known to put in place these compliance programs, you can help your employees. If they're able to say to people they deal with overseas, “Look, I cannot do this. I will get fired and I'm being watched. Everything I do is

being periodically audited. And we all have a duty to report this. So, it's just a no go." That's a lot better than the employee not being able to point to the entire corporate culture being against it. And that word does spread. And [there is] the availability of NPAs, which Wally will touch on. Very quickly, let me throw it to Frank to touch on some specific acquisition-related issues.

FRANK EICHLER: Thanks Ross, and again, they're listed here. I think you have to go through the interview. I think you have to review the internal policies. A lot of companies will not have anything. I think, most importantly, again, if you're in one of those red countries, make sure you engage local counsel [and] local auditors who, again, have a knowledge of some of the local procedures and policies and things that take place. You just really [need] to make sure when you do an acquisition—because again, once you've closed it, if there's an FCPA problem, the DOJ says, "That's your problem." So again, if you do the normal things, including it in the documents and everything else, but you really need to do that real tough review and make sure you've found everything out that you can find before you close.

ROSS BOOHER: Great. And here's just three quick snapshots of problems—examples of problems. The top one is a recent one. In that instance [eLandia] spent—I think it was—approximately \$26 million to acquire Latinode, and discovered it had some problems. eLandia handled the matter in a really comprehensive way that drew praise from the DOJ, and, as a result, eLandia was never sanctioned. But, as a result of the overall problem they had essentially purchased, they had to write down that \$26 million approximately investment by \$21 million. So, that is an example of the type of problem that can occur. In that instance, eLandia went in, they did a thorough investigation, they fired the people who were problems, they shut down business operations, and they self-disclosed to the government, and that was the way they protected eLandia. But still, obviously, they had to spend an awful lot, no doubt, to fix that problem.

So, now turning further to Wally for the issue of: If a company discovers a problem [via a] hotline report, during an audit, etc., Wally, what is the next step?

WALLY DIETZ: Very briefly, because we need to save some time for questions, it's like any other internal investigation.

Very briefly, to save some time for questions, I'll just summarize this in a few seconds. You have to put together the right team, involving your in-house counsel, your auditors, your external auditors. You have to consider using outside general counsel to lead the team. Protecting the privilege, as you know, in any investigation is really important. And again, because it involves statutes, by definition in two countries, you have to select a law firm not only in the U.S. that knows the law, but a very good firm in the foreign jurisdiction where the question arises. And again, that's where we have utilized our Lex Mundi partners repeatedly on these types of issues.

ALEXANDRA WRAGE: Great, thank you. If I could pause for just a moment and see if there are any questions from the audience. We've had one or two that I think we've answered in the course of the presentation, although there's one that I'll add just now. But please do take a moment if you're online and you have questions that you send them to us electronically and we'll endeavor to respond to them.

One that came in a little bit earlier that I'm just going to cycle back to very quickly is: Somebody asked the question, "What about nongovernmental employees?" And I'll just take a quick stab at this. If they're truly nongovernmental employees—they're truly not foreign officials as very broadly defined under the FCPA—then the FCPA just doesn't apply to them. It doesn't mean, as we heard earlier, that other laws won't. And there's a sort of movement afoot to harmonize rules within companies for private-to-private bribery—pure commercial bribery. We've done a lot of benchmarking on that, as well as the bribery of government officials. But the trickier part of that is—the example that was given and the question is—"What about employees of utilities?" In so many countries, it takes longer to assess whether somebody is technically a government official than to just respond as if they were. So, we see a lot of companies default to the position that they should just all be treated as government officials, because it's just faster and safer and, frankly, very often less expensive. I wonder if any of the panelists wanted to add to that.

ROSS BOOHER: I think that's exactly right. This is Ross. That is one of the big issues: Are your employees actually dealing with government officials, or people that the DOJ, and under the FCPA, are going to be considered foreign officials. And a lot of times we deal with clients and they think that they are not, but in fact they are, and it can be anyone from customs officials, or dealing with a state-owned airline, hospitals, you name it. And part of the front-end process, and what you want to make sure your compliance program addresses, is that when you are entering a market, or if you're getting up to speed on the market from an FCPA perspective, that that is part of your risk assessment. You look at your manufacturers, you look at your vendors, you look at who they're dealing with, and you determine, "Are we dealing with foreign officials as it's defined under the act?" And, as Alexandra said, a lot of companies are just going to say, "You know what? We're just going to require our employees to treat everyone as though they're a foreign official," and that's the safest course of action.

FRANK EICHLER: I'll add to that. We did an acquisition here in the last two years in China and we were told they were not government officials, they were not anything else, [and] everything was fine; they were employees. Three weeks later, after we'd done a lot more work, we found out they would be deemed to be government officials and we ran—not walked—away from that one. You've just got to be very, very careful.

ALEXANDRA WRAGE: Right, thank you. And just to keep us moving along in the remaining moments that we have, let's cycle back a little bit to self-disclosure and talk a little bit more about the benefits and risks. We're all pretty familiar with the risks, but perhaps emphasizing the benefits of self-disclosure.

WALLY DIETZ: This is Wally Dietz. There are some benefits. Obviously, it puts you in a favorable light with the government and it may result in leniency. Despite the large nature of the fines in Siemens, in fact, the government felt like Siemens cooperated extensively with the investigation and the fines could have been significantly more than they were. It's just a matter of approaching the government and starting off on the right foot, and then you can direct the discussions from there.

But the biggest mistake a client can make or a company can make is to call the government and say, "We think we've got a very small problem: this minor payment to this agent or this foreign official." And the government, before they go anywhere else, they're going to ask questions. What is your compliance program? How do you enforce it? How do you know this is not a larger issue than you're talking about? And so, it is a big mistake to call the government and self-report until you have conducted a complete and thorough investigation of the situation so you know all the facts. Just as Frank related a moment ago, sometimes things are not exactly as they seem.

ROSS BOOHER: And just to add: This is the reason for the compliance program. One, the goals are: You want to prevent problems, you want to detect them early, and you want to be able to isolate and address them. And if you have a good program in place, you're going to be able to quickly answer the questions that are up there on the screen, and be able to do so with confidence, and not have to worry about a number of other shoes dropping. It'll be much less likely that would occur.

ALEXANDRA WRAGE: All right. Thank you. Let's move to the next slide then. And Frank, if you could talk us through the next two slides? Thanks.

FRANK EICHLER: Sure, and again, these are on the slides. How are your employees looking at it? How would they describe the program? What are the questions that the enforcers are going to ask? One thing to remember: This will always be done in hindsight. I can't emphasize that enough. Think of yourself as if you are the investigator asking after something has been disclosed. You're going to have to say whether the compliance program is tailored to the business activity [and] foreign jurisdiction, and are the employees not only asking the questions but also are they also raising it to the next level, so that we can hear about it as the compliance officer.

ALEXANDRA WRAGE: Excellent. Thank you. I think that's great advice and it's very helpful to hear it from somebody who is in-house. I'm going to pause one more time for questions.

*[The CLE code and instructions provided here were for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast when you have finished listening to it, click the EXIT COURSE button at the top right of the screen to return to your My Courses page and then click the certificate link or icon beneath the course listing. In the pop-up window, select the desired jurisdiction from the drop-down list and enter any requested data, such as your bar number and the CLE code that popped up while you were playing the archived webcast. (This code is required for New York and Ohio attorneys only.)]*

ALEXANDRA WRAGE: Right. Thanks so much, and we've heard a great deal about what an incredible resource Lex Mundi law firms worldwide can be, but Ross and Wally, can you talk to us about some of the other resources that are available?

ROSS BOOHER: Yes, there is the Web address for Lex Mundi, obviously, and I think attached to the registration was the Best Practices Guide. Many of the items that we discussed today are contained in there. I would definitely recommend that to you. But also, I'll mention to you Alexandra's blog. Her organization, TRACE International, is an outstanding organization, and Alexandra's blog—the is address up there—has a lot of compliance information. It's updated regularly, and as a practitioner I can tell you that I use it and look it on almost a daily basis. So I would commend that to everyone as a tremendous resource.

ALEXANDRA WRAGE: Thank you so much. And we see resources listed for your law firm, as well, that we encourage everybody to check out. Just for clarification then, I am with TRACE; we're a nonprofit business association that helps companies with antibribery compliance tools and services. The map of the world you saw earlier showing where the risk is internationally is a product that is put out by Transparency International and a lot of companies rely on.

So, with that, we don't have additional incoming questions, although on the final slide I believe you're going to see the e-mail addresses of the panelists who have participated today and everyone has invited people with follow-on questions to contact them with those questions. So, all that remains then is for me to thank Lex Mundi for their sponsorship of this event, and to encourage people to find them at the annual meeting in Boston, and to thank our panelists, Wally Dietz, Ross Booher and Frank Eichler, for a really fabulous presentation. And with that, we will conclude the webinar. Thank you.

ROBERTO SCALESE: Thank you, Alexandra. On behalf of the Association of Corporate Counsel and SmartPros Legal and Ethics, thank you all again for listening to today's program.

*[The CLE code and instructions provided here were for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast when you have finished listening to it, click the EXIT COURSE button at the top right of the screen to return to your My Courses page and then click the certificate link or icon beneath the course listing. In the pop-up window, select the desired jurisdiction from the drop-down list and enter any requested data, such as your bar number and the CLE code that popped up while you were playing the archived webcast. (This code is required for New York and Ohio attorneys only.)]*

Thank you again. This program is now concluded. Have a great day.