Avoiding Legal Peril:
Tips for Simulation Companies Dealing with Governments

Edmund T. Baxa, Jr.
Partner
Orlando, Florida
Foley & Lardner LLP
ebaxa@foley.com

Michael P. Matthews
Partner
Tampa, Florida
Foley & Lardner LLP
mmatthews@foley.com

David W. Simon
Partner
Milwaukee, Wisconsin
Foley & Lardner LLP
dsimon@foley.com

ABSTRACT

With a customer base that is heavily government-oriented, companies in the MST industry operate in a sphere of increasing legal risk. The U.S. government has stepped up its pursuit of government contractors domestically through the False Claims Act (FCA) and internationally through the Foreign Corrupt Practices Act (FCPA). As many companies have discovered, these aggressively enforced laws can present traps for the well-intentioned but unwary. Understanding the FCA and the FCPA is essential for any person or company doing business with a governmental entity. This paper provides an overview of those legal risks and provides practical guidelines, which, if followed, minimize those risks.

The FCA creates liability (and a potential cause of action for whistleblowers) whenever a company submits a false claim to the government, makes a false statement that causes the government to pay a claim, or keeps government money that it is not entitled to retain. Investigations of potential fraud at such companies can result in multi-million dollar settlements and judgments, debarment/exclusion from doing business with the government, and criminal sanctions, including prison for individuals and substantial fines for companies.

While the False Claims Act governs domestic activity, the FCPA addresses a company's dealings with foreign governments. Covering far more than the traditional notion of a suitcase full of cash paid to a ministry official in exchange for a big government contract, the FCPA criminalizes corruptly providing "anything of value" to any "foreign official" in order to obtain or retain business or an improper advantage. Corporate fines imposed pursuant to the statute have been staggering, regularly reaching into the hundreds of millions of dollars.

The paper will provide an overview of the laws, their potential application, and enforcement trends, as well as detailed guidance on how companies can minimize risk through effective compliance programs, internal controls, and human resource policies.

ABOUT THE AUTHORS

Edmund T. Baxa, Jr., is a member of the Government Enforcement, Compliance & White Collar and the Life Sciences Industry Team. He has assisted healthcare, commodity trading, transportation and construction companies in internal and external investigations involving allegations of securities fraud, Medicare/Medicaid fraud, breaches of fiduciary duty and bid rigging. He has defended clients in federal criminal cases concerning the importation and transportation of hazardous substances. Mr. Baxa has also represented clients in connection with grand jury investigations of labor racketeering and tax/customs violations. Mr. Baxa has tried over 30 cases to juries and has represented numerous clients before arbitration panels and various Federal and State agencies.

Michael P. Matthews is vice chair of Foley & Lardner's Government Enforcement, Compliance & White Collar Defense Practice. Mr. Matthews is a litigator with experience in securities class actions, SEC enforcement matters, and shareholder derivative actions, including several of the largest such matters in U.S. history, as well as False Claims Act and other government enforcement and complex litigation matters. Mr. Matthews conducts internal investigations in the U.S. and abroad on behalf of corporations, audit committees, special litigation committees, and boards of directors. He has represented clients in a variety of federal and state False Claims Act cases.

David W. Simon is a partner in the Government Enforcement, Compliance & White Collar Defense; Securities Enforcement & Litigation; and Antitrust Practices. He is a litigator with substantial experience conducting internal in-

vestigations, defending corporations in government enforcement actions, and representing corporate clients in state and federal courts. He devotes much of his practice to helping corporate clients manage crises that potentially give rise to government enforcement actions. His FCPA experience includes conducting an internal investigation into potential FCPA violations arising out of the business practices of a client's agent in Indonesia; and representing a manufacturing client in connection with FCPA issues arising out of a former subsidiary's business practices in China.

Avoiding Legal Peril: Tips for Simulation Companies Dealing with Governments

Edmund T. Baxa, Jr.
Partner
Orlando, Florida
Foley & Lardner LLP
ebaxa@foley.com

Michael P. Matthews
Partner
Tampa, Florida
Foley & Lardner LLP
mmatthews@foley.com

David W. Simon
Partner
Milwaukee, Wisconsin
Foley & Lardner LLP
dsimon@foley.com

UNDERSTANDING THE FCA AND THE FCPA

With a customer base that is heavily government-oriented, companies in the military simulation and training ("MST") industry operate in a sphere of increasing legal risk. The U.S. government has stepped up its pursuit of government contractors domestically through the False Claims Act ("FCA") and internationally through the Foreign Corrupt Practices Act ("FCPA"). As many companies have discovered, these aggressively enforced laws can present traps for the well-intentioned but unwary. Understanding the FCA and the FCPA is essential for any person or company doing business with a governmental entity, including system integrators, contractors and companies in the military simulation and training field. This paper provides an overview of those legal risks and provides practical guidelines, which, if followed, minimize those risks.

The FCA could create liability for a company in the MST industry (and a cause of action for whistleblowers) if it submits what is deemed to be a "false claim" to the government, makes a false statement that causes the government to pay a claim, or keeps government money that it is not entitled to retain. Any company that does substantial business with the U.S. government has significant exposure under this law. Investigations of potential fraud at such companies can result in multi-million dollar settlements and judgments, debarment/exclusion from doing business with the government, and criminal sanctions, including prison for individuals and substantial fines for companies.

While the False Claims Act governs domestic activity, the FCPA addresses a company's dealings with foreign governments and their instrumentalities. Companies in the MST industry that do business or have contracts with foreign governments should beware. Covering far more than the traditional notion of a suitcase full of cash paid to a ministry official in exchange for a big defense contract, the FCPA criminalizes corruptly providing "anything of value" to any "foreign official" in order to obtain or retain business or an improper advantage. Corporate fines imposed pursuant to the statute have been staggering, regularly reaching into the hundreds of millions of dollars.

The paper will provide an overview of the laws, their potential application, and enforcement trends, as well as detailed guidance on how companies can minimize risk through effective compliance programs, internal controls, and human resource policies.

The U.S. False Claims Act

Government contractors in the MST industry should be aware of potential exposure presented by the federal False Claims Act, as well as actions that can be taken to reduce the risk of such exposure. Although the FCA is essentially a fraud statute aimed at combating false claims and false statements submitted to the government, its application takes many forms -- not all of which are entirely obvious, yet which can trigger massive liability because of treble damages and penalties available to the government and whistleblowers under the FCA, in addition to the threat of suspension and debarment that oftentimes accompany such claims.

As an example, in one FCA case, a military flight simulator manufacturer was required under applicable federal contracting regulations to submit its best estimate of the costs that would be incurred in performance of the contract to the government. A government auditor discovered that the simulation company maintained two sets of estimates, one showing its best estimate and another which included an allegedly "padded" amount of typically 7-10%. The latter estimate was submitted to the government as the simulation company's best estimate, which the government alleged was done fraudulently to inflate the government's cost and the company's profit, to the tune of $77,000,000 – which when trebled would be $231 million. After being sued under the FCA, the company settled the case for over $50,000,000. Although there are few reported FCA cases thus far filed against companies and individuals in the MST industry, the growth of the industry and its reliance on government contracting, as well as recent legislation that expands the types of cases that may be brought under the FCA, virtually

guarantees that an increase in the number of industry participants targeted under the FCA is on the horizon.

Overview of FCA

Although the False Claims Act is used most frequently in connection with health care fraud, the FCA has deep roots in defense contracting. With its first iteration enacted in 1863, "the principal goal of [the FCA was] 'stopping the massive frauds perpetrated by large [private] contractors during the Civil War.'"[i] Since then, the FCA has been amended to further the goal of the FCA "to protect the funds and property of the Government from fraudulent claims, regardless of the particular form, or function, or the Government instrumentality upon which such claims were made." *Rainwater v. United States*, 356 U.S. 590, 592 (1959).

In 1986, Congress amended the FCA in response to a perceived increase in defense industry fraud.[ii] The purpose of the 1986 amendments was to transform the FCA into a more potent tool against modern fraud by incentivizing whistleblowers with non-public information to come forward and alert the Government that it was being defrauded.[iii] Not only was the percentage of the reward to be shared with the relator increased, the potential liability was also substantially increased. Since then, the FCA has been used to recover over $22 billion.[iv]

Most recently, the FCA has been amended by the 2009 Fraud Enforcement and Recovery Act, and again as part of the Patient Protection and Affordable Care Act of 2010 – in neither instance to protect government contractors, but instead to expand the ability of the Department of Justice and whistleblowers to bring FCA claims. The 2009 amendment, for example, broadened the definition of "claim" under the statute so that the submission of the claim need not result in an immediate demand on the United States Treasury, making clear that a subcontractor submitting a false claim to a prime contractor to obtain payment from the prime contractor may give rise to an FCA claim if the prime contractor is using government funds or advancing the government's interest. The 2010 amendments narrowed the "public disclosure bar" that prevents whistleblowers from trying to recover for asserting allegations that have already entered the public domain through certain channels.[v]

False claims liability can arise under two different code sections, covering both criminal and civil liability. Under 28 U.S.C. § 287, the criminal statute, a person who presents a false claim to the government knowing it to be false shall be imprisoned up to five years and subject to fines. Under the civil False Claims Act, 31 U.S.C. §§ 3729-3733, those who knowingly submit, or cause another person or entity to submit, false claims for payment of government funds are liable for three times the government's damages plus civil penalties of $5,500 to $11,000 per false claim. False claims matters are more frequently initiated under the civil statute, largely because of the monetary incentive for whistleblowers to initiate suits, as well as the lower burden of proof and more forgiving "deliberate ignorance" or "reckless disregard" standard versus knowledge of falsity required under the criminal statute.

Under the FCA, actions may be instituted by the Attorney General or by a whistleblower, referred to as a qui tam relator, who would bring the action on behalf of the Government. Because the private individuals must have independent knowledge of non-public allegations, the relator is most often "an insider at a private company [who] brings an action against his own employer."[vi] Under 31 U.S.C. § 3730(d), the relator is entitled to share in the proceeds of any action. An innocent relator may receive at least 15 percent but no more than 25 percent if the government intervenes or between 25 percent and 30 percent if the government does not intervene (culpability of the conduct alleged can reduce the relator's recovery). To put this in perspective, consider the military flight simulator example described above. 15-30 percent of $50,000,000 is between $7,500,000 and $15,000,000, and represents a significant motivational factor for any defense contractor employee, regardless of their employment level or years of experience. In addition, the government has the advantage of building one-sided cases during the period when the complaint remains under seal, while the government decides whether to intervene.

Types of False Claims Act Violations

The core subsection of the civil FCA provides for penalties and treble damages for seven different types of violations, by any person who:

> (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;
>
> (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;
>
> (C) conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G);
>
> (D) has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property;

> (E) is authorized to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely knowing that the information on the receipt is true;
>
> (F) knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge property; or
>
> (G) knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government.

The most common FCA provision alleged to be violated is subsection (A) above, for presenting or causing another to present a claim for approval knowing the claim to be false. Subsection (A) is the most straightforward of the subsections, the one used for the most common allegations such as those of overbilling, billing for work not performed, upcoding or upcharging, etc. Such allegations likely would not be much different for someone in the MST industry than any other government contractor, as in the example above involving the military flight simulator manufacturer.

Subsection (B) is also commonly invoked, as it prohibits not just false claims themselves, but false statements material to false claims. A growing number of actions have been based on a "false certification" theory by which it is alleged that the submission of a claim which expressly or impliedly certifies compliance with a federal statute, regulation, or contract term when the same has not been complied with renders the claim false or fraudulent, even though the claim itself is not facially false. Such claims continue to be asserted against defense contractors for providing technology that did not perform as promised. Recently, the U.S. District Court for the Middle District of Florida denied a defense contractor's motion to dismiss a complaint which alleged a false certification FCA claim.[vii] In the complaint, the relator alleged, among other things, that the defendant violated the FCA by submitting or causing to be submitted claims for payment despite the fact that the defendant had falsely certified on each box of grenades that the grenade components were performing properly and safely.

For a MST contractor, this could take a variety of different forms, not all of which intuitively seem to involve fraud. Although the FCA is not intended to be used to enforce compliance with regulations and contract provisions, FCA claims could arise from failure of simulators to meet specs -- particularly if there are performance specs involved, e.g., that the simulator will accurately replicate real life conditions so as to provide effective training. For example, if a medical simulator intended to train battlefield medics on the application of tourniquets to slow or stem bleeding delivers training that is not in accordance with current battlefield medicine practices, or does not thoroughly train the medic in all proper procedures and protocols, FCA claims might be asserted based on certification of capabilities or failure to meet underlying performance specs.

Even less obvious FCA violations can be alleged where the false certification is not express, but only implied. "The theory of implied certification . . . is that where the government pays funds to a party, and would not have paid those funds had it known of a violation of a law or regulation, the claim submitted for those funds contained an implied certification of compliance with the law or regulation and was fraudulent."[viii] For example, if a MST contractor gives a government official something of value and the government decides it is an illegal kickback, the government may seek to argue that it would never have paid the contractor's claims had it known the contractor was paying kickbacks, and therefore the claims submitted were false claims, even if the contractor did not submit the claims with an express certification that it did not pay any kickbacks. Implied certification is not universally accepted and in many instances, courts have restricted its application to situations in which the government's payment was explicitly conditioned, albeit not within the contract, upon certification of compliance with a specific statute or regulation.[ix] Under both implied and express certification theories, the whistleblower must prove that the alleged violation of the underlying statute, regulation, or contract term occurred before FCA liability can be imposed. So-called "reverse" false claims causes of action, under subsection (G) above, are also fairly common, as are conspiracy claims under subsection (C), often as an add-on claim to claims under subsections (A) or (B).

Reducing the Risk of FCA Liability

There are a number of steps that government contractors in the MST industry can take to reduce the risk of an FCA violation. First, perform a risk assessment, gathering as much information as you can about what services you offer or products you make that are eventually sold to the government (this article focuses on

the federal FCA, but states also have their own versions of the FCA that may apply). Also gather information about any and all certifications made to the government, either in formal, written proposals or claim submissions, or even in informal communications with the government. Often FCA cases are brought based on a number of certifications, including annual or other periodic certifications as well as certifications submitted with each claim. This may also include requests for change orders or extensions of time. Remember that the certifications need not actually accompany a claim to be actionable, because even if they are not submitted for payment, if the statements are false and cause a later claim to be false, FCA liability can attach. Consult with legal counsel before retaining overpayments from the government, as doing so can create liability under the reverse false claims provisions of the FCA.

Additionally, both training of employees and having an effective compliance program help reduce the risk of FCA claims. It is important that these compliance programs be more than just pieces of paper; they should be robust, active programs woven through the fabric of the organizations. They should include components such as a hotline that employees are encouraged to use to report fraud. In addition, a compliance-oriented tone should be implemented from management down through the organization. Tell employees to monitor any and all work to insure that any certifications of compliance with any statute, regulation, or contract term are accurate and truthful. Have the employees sign documents confirming that they have read and will follow the policies and procedures. Regularly test employees involved in government billing on knowledge of the policies and rules. Establish protocols, such as anonymous reporting, to encourage employees to come forward with concerns. Audits may also assist in identifying fraud risk areas or non-compliance that risks FCA liability.

Another step is to obtain information from exiting employees. A detailed exit interview can provide valuable information as to any concerns the employee has. Moreover, if the employee indicates that they have no concerns, have the employee sign a statement to that effect. Although this would not insulate you from a later FCA case, it would call into doubt the employee's credibility. Similarly, formal severance agreements can help limit potential exposure. First, the severance agreement should require the employee to divulge any wrongdoing or to represent that he or she is not aware of any wrongdoing. Moreover, some courts have not enforced agreements not to bring FCA cases, a number of courts have enforced provisions that reduce the potentially enticing financial incentives for employees to file FCA claims, for example, contracts providing that if the employee brings a FCA case, he or she agrees to dismiss the case if the government chooses not to intervene.[x]

The FCA also has anti-retaliation provisions under which employers can be held liable for retaliating against employees who complain about conduct violating the FCA. Needless to say, employers should consult legal counsel before demoting, firing, or taking any other adverse action against employees who have reported conduct that may violate the FCA. Likewise, MST companies that become aware of potential misconduct by employees that may violate the FCA should consult legal counsel about performing an internal investigation and possibly self-reporting violations to the government.

The FCA can trigger enterprise-threatening liability, sometimes in the tens of millions or even hundreds of millions of dollars. MST companies whose services or products are sold to the government should be aware of such risks and take steps to reduce them before the risks materialize.

THE FOREIGN CORRUPT PRACTICES ACT

On January 18, 2010, federal agents raided the Shot Show trade show in Las Vegas.[xi] The raid resulted in the arrest and indictment of 22 executives and employees of companies in the military and law enforcement products industry for alleged violations of the FCPA.[xii] Those arrested included employees of both large and small companies; private companies and publicly traded companies; chief executives, sales managers, and a general counsel.[xiii] In a press release issued shortly after the raid, the DOJ characterized the raid as the "largest single investigation and prosecution against individuals in the history of the DOJ's enforcement of the FCPA."[xiv] The unprecedented breadth and scope of the raid confirmed that the broader defense industry, of which the MST industry is a part, remains a primary target of FCPA enforcement actions, and that companies and individuals operating within that industry must take significant, affirmative steps to minimize their exposure to criminal liability under the FCPA. Since many companies that develop and sell modeling and simulation technologies operate within the defense industry, these companies are equally vulnerable and, accordingly, must be especially careful in their business dealings outside the United States. Given the government's increased enforcement of the FCPA across all industries, those companies whose modeling and simulation business may not be primarily defense-related should nevertheless take steps to ensure

that any business dealings outside the United States do not result in exposure to criminal liability.

The FCPA Explained

The FCPA is the U.S.'s foreign antibribery law enforced by both the DOJ and Securities and Exchange Commission ("SEC").

The FCPA presents numerous traps for the unwary. Conduct that to many may appear innocent, may in fact subject U.S. companies and citizens doing business abroad to hefty fines reaching in the millions, and sometimes even the hundreds of millions, possible debarment, and other equally harsh penalties. Those wishing to protect themselves from unintended violations of the law must familiarize themselves, not only with the statutory language, but with the manner in which the law is construed and enforced by the DOJ and SEC.

The FCPA has two main provisions: the Antibribery Provision and the Books and Records Provision.[xv]

The Antibribery Provision. The FCPA's Antibribery Provision applies to (a) all U.S. companies and citizens; (b) foreign companies listed on a U.S. stock exchange; or (c) any person who commits a prohibited act while in the United States.[xvi] The provision specifically prohibits these companies and individuals from corruptly paying or offering to pay, directly or indirectly, money or *anything of value* to a *foreign official* for the purpose of *obtaining or retaining* business.[xvii] The danger for the uninitiated lies in the government's broad interpretation of the terms "anything of value," "foreign official" and "obtaining or retaining." These broad interpretations criminalize much more than the traditional "suitcase full of cash" notions of bribery.

The term "anything of value" has been construed to include not only cash or a cash equivalent, but also, among other things, discounts; gifts; use of materials, facilities, or equipment; entertainment; meals; transportation; lodging; insurance benefits; and the promise of future employment. There is no de minimis value associated with the "anything of value" element, and the perception of the recipient and the subjective valuation of the thing conveyed is often a key factor considered by the enforcement agencies in determining whether "anything of value" has been given to a foreign official. For example, MST contractors may run afoul of the FCPA's "anything of value" element in situations where they pay for a foreign officials' expenses in traveling to meet with the contractor to view a demonstration of simulation equipment if the expenses are deemed excessive or the visit includes non-business activities.

The term "foreign official" has been interpreted to include not only traditional government officials, but also employees of state-owned or state-controlled entities ("SOE") under the theory that SOEs are an "instrumentality" of the foreign government. Even if a foreign company is not wholly-owned by a foreign state, it may still be considered an "instrumentality" of the foreign government if the foreign government exercises substantial control over the entity.

The Shot Show Sting, referenced earlier, is a prime example of the danger that the Government's interpretation of the term "foreign official" poses to those in the MST industry. The Shot Show Sting resulted in the indictment of 22 individuals, and demonstrates the government's increased willingness to (a) use undercover law enforcement tactics to uncover alleged FCPA violations; and (b) prosecute individuals for FCPA violations. Trials of the various individuals indicted in this sting operation are currently ongoing.

The defendants in the Shot Show case are accused of attempting to bribe Gabon's defense minister, through their dealings with the undercover agent, for the purpose of securing contracts for the sale of military and law enforcement equipment to outfit Gabon's Presidential Guard.[xviii] Significantly, although the FCPA targets' corrupt conduct was aimed at influencing a "foreign official," there was no actual "foreign official" in the Shot Show case. It was a sting operation. The defendants believed they were doing business with an advisor to Gabon's defense minister, when in fact they were dealing with an undercover FBI agent.[xix] The agent met with the defendants at the Washington restaurant Clyde's and spoke individually to the defendants on the balcony of the restaurant.[xx] These conversations were recorded by the FBI using hidden cameras and microphones.[xxi]

The "obtain or retain business" element of the Antibribery provision also has broad application and will be satisfied even if the improper payment to a foreign official does not lead to a government contract. Courts have held that Congress, by passing the FCPA, intended to prohibit a wide range of improper payments, not just those that directly influence the acquisition or retention of government contracts. Indeed, several recent FCPA enforcement actions concern improper payments to a foreign official to secure special tax or custom treatment, to secure government licenses or permits needed to do business in a foreign jurisdiction, or otherwise to secure an improper advantage over competitors. MST contractors may unintentionally run

afoul of the FCPA's "obtain or retain business" element when dealing with customs issues in shipping their simulation equipment overseas or in having parts shipped into the United States or other countries that will be used to assemble the equipment.

The Books and Records Provision. The Books and Records Provision requires "issuers" to keep books and records that accurately reflect business transactions and to maintain effective internal controls (the "Books and Records Provision").[xxii] An "issuer" constitutes any company (including foreign companies) with securities traded on a U.S. exchange or otherwise required to file periodic reports with the SEC. While the Books and Records provision technically applies only to issuers and not to foreign subsidiaries, the enforcement agencies routinely hold parent companies liable for false or fraudulent entries on any book or record of the parent's subsidiary that is ultimately consolidated with the parent's books and records for financial reporting purposes. In many instances, improper payments to a foreign official to obtain or retain business result not only in Antibribery charges, but also Books and Records charges, given that improper payments are often falsely characterized on a company's books and records as "miscellaneous" expenses, "commissions," etc. and given the enforcement agencies' view that the improper payments would not have been made if the company had effective internal controls.

Fines and Penalties. FCPA enforcement has become a profitable business for the government. Last year the government collected $1.4 billion in combined fines and penalties from 20 separate FCPA enforcement actions.[xxiii] Last year also saw the imposition of the longest prison sentence to date for an individual prosecuted under the FCPA.[xxiv] In April 2010, Charles Paul Edward Jumet received a sentence of 87 months.[xxv] Given that prior prison sentences for FCPA violations tended to average 1 year, Jumet's sentence may signal an increased willingness by judges to hand down harsher penalties to individuals convicted of violating the FCPA.

Such fines and penalties are in addition to harsh collateral sanctions that can result from an FCPA violation, including (a) termination of government licenses; and (b) debarment from government contracting programs. In addition to the above fines and penalties, the SEC is also able to seek disgorgement of a company's profits on contracts secured with improper payments. Further, enforcement agencies often seek appointment of an independent compliance monitor over FCPA corporate violators for multi-year periods, a process which can be cumbersome and expensive for companies.

Risk of Liability for Acts of Third Parties, Subsidiaries, and Joint Venture Partners

Under the FCPA, the actions of foreign subsidiaries and other third parties (such as agents, consultants, distributors, joint venture partners, etc.) can result in FCPA liability to a parent company or the entity engaging the third-party. In other words, companies are not immune from FCPA liability by doing business abroad through others. Indeed, many recent FCPA enforcement actions are based not on conduct directly engaged in by a company, but rather conduct engaged in by various third parties on behalf of a company.

Under the FCPA, knowledge is defined broadly and is present when one knows that an event is certain or likely to occur. Further, failing to take note of an event or being willfully blind can also constitute knowledge.

The enforcement action brought against United Industrial Corporation ("UIC") serves as a good example of how dealings with third-party agents and contractors poses significant risks under the FCPA. In 2009, UIC resolved an FCPA enforcement action brought by the SEC by agreeing to pay a total of $337,679.42 in penalties.[xxvi] UIC, a Delaware corporation headquartered in Maryland, focused on the design and production of defense, training, transportation and energy systems for the U.S. Department of Defense and domestic and international customers.[xxvii] The enforcement action was based on the acts of one of UIC's indirect wholly-owned subsidiaries, ACL Technologies, Inc. ("ACL").[xxviii] Specifically, the enforcement action targeted payments made by ACL to a third-party agent in connection with ACL's contract under the U.S. Foreign Military Sales Program to build a depot for F-16 combat aircraft for the Egyptian Air Force, and to provide, operate and train Egyptian labor to use the testing equipment installed in the depot.[xxix] In 1996, ACL's President, Thomas Wurzel, hired the third-party agent, a retired Egyptian Air Force general, to help move the depot project forward.[xxx] The SEC alleged that Wurzel authorized ACL to make payments to the Egyptian agent while knowing or consciously disregarding the high probability that the agent would offer, provide or promise at least a portion of such payments to EAF officials for the purpose of awarding business to ACL and UIC.[xxxi] In a related enforcement action, Wurzel, without admitting or denying the charges, agreed to pay a $35,000 civil penalty.[xxxii]

In its complaint against UIC, the SEC noted that, although UIC had instituted policies in 1999 outlining procedures for retaining, and working with, foreign agents, ACL failed to follow those procedures.[xxxiii] Specifically, ACL failed to conduct any due diligence

on the Egyptian agent for a period of seven years despite UIC policy which required ACL to submit due diligence forms to corporate counsel prior to engaging the agent.[xxxiv] ACL also failed to include FCPA clauses in the agent's contracts, despite UIC policies requiring such clauses to be included.[xxxv]

Recent Enforcement Trends

Increased Enforcement Generally. FCPA enforcement has become a primary focus for both the DOJ and SEC. At a conference in November 2010, Lanny A. Breuer, the Assistant Attorney General for the DOJ's Criminal Division stated: "I'm proud to say…we've imposed the most criminal penalties in FCPA-related cases in any single 12-month period – ever. Well over $1 billion."

The SEC has also dramatically increased its enforcement activity. In 2008, eleven entities were subject to SEC enforcement actions. In 2009, ten entities were subject to enforcement actions. In 2010, eighteen entities and seven individuals were subject to enforcement actions. Moreover, in 2010 the SEC established a specialized unit devoted entirely to the prosecution of FCPA cases. Given the government's ability to collect exorbitant penalties from companies accused of FCPA violations, all indications point to the continued rise in FCPA-related enforcement actions.

Other Enforcement Trends. Both the DOJ and SEC have begun to focus on investigating and targeting industries as a whole, rather than specific companies. In targeting particular industries, the government will likely investigate, and act on, information it obtains about or from a target company's competitors.

The prosecution of individual officers and employees for FCPA violations is also becoming increasingly prevalent. While the DOJ had prosecuted fewer than 10 individuals between 2005 and 2007, the DOJ prosecuted 10 individuals in 2008, over 15 in 2009, and over 25 in 2010, which included the 22 individuals indicted in the Shot Show case. Also becoming more prevalent is the government's use of traditional under-cover law enforcement techniques, including the use of undercover agents and wiretaps.

Another significant trend is the U.S. government's increased cooperation with its foreign counterparts. The enforcement agencies are actively working to foster strong relationships with law enforcement colleagues overseas. This increased cooperation will make it much easier for the U.S. government to obtain evidence from foreign law enforcement and to prosecute FCPA violations.

Lastly, the United States is not the only country targeting corruption. Last year the United Kingdom passed anti-corruption legislation that is broader in scope that the FCPA. Accordingly, any company doing business in the United Kingdom must become familiar with this new legislation. In addition to the United Kingdom, many other countries around the world, including Russia and China, have begun to target and prosecute corruption. Accordingly, it is imperative for companies to be familiar with the laws governing the countries where they do business.

Guidelines for Minimizing FCPA-Related Risks

Given the realities of the international marketplace, it is virtually impossible for an MST company doing business abroad to completely insulate itself from all possible exposure to liability under the FCPA. However, the following steps, if taken, greatly minimize the risks of exposure:

Implement Effective Compliance and Training Programs. The easiest and most important step an MST company can take to minimize its exposure under the FCPA is to establish an effective anti-corruption compliance and training program. It is critical that steps are taken to actively enforce, and periodically review the effectiveness of, the program. Companies that have a compliance program "in name only" will not be looked upon favorably by the government.

Any truly effective compliance should begin with an assessment of FCPA risk and a clearly articulated corporate policy addressing that risk. In assessing FCPA risk, MST companies should especially consider where they do business (and the pervasiveness of corruption in those countries), who their customers are (foreign governments or SOEs?), and how they go to market, especially if they use agents and brokers to represent their interests abroad.

In addition to a clearly articulated anti-corruption policy, MST companies should promulgate standards and procedures designed to detect and deter violations of the FCPA and other anti-corruption laws, and should otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance.

The FCPA policies, standards, and procedures should apply to all directors, officers, and employees, and certain business partners in foreign jurisdictions such as agents, consultants, representatives, distributors, and joint venture partners. Directors, officers, employees, and Third Parties should be required to certify annually and in writing that the signing party: (a) has read, un-

derstands, and will comply with the company's FCPA policies, standard, and procedures; and (b) has not participated in any unreported or prohibited transactions or activities within the reporting period, and knows of no prohibited activity by any other director, officer, employee, or Third Party.

The board of directors (or other governing authority) should have overall responsibility for the compliance program and must remain knowledgeable about the content and operation of the program. One or more senior corporate officials within the organization should have day-to-day responsibility for the implementation and oversight of the FCPA policies, standards, and procedures. The person(s) responsible for the day-to-day compliance program must be given adequate resources and authority, must periodically report to senior officials within the organization and the board of directors, and must be given direct access to the board of directors (or a designated sub-group such as an audit committee).

Mechanisms should be designed to ensure that FCPA policies, standards, and procedures are effectively communicated to all directors, officers, employees, and third parties. Such mechanisms should include (a) periodic training; and (b) periodic written communications concerning the requirements of the FCPA.

Conduct Appropriate FCPA Due Diligence. Prior to entering into an agreement with an agent, broker, distributor or joint venture partner, MST companies should conduct appropriate due diligence to determine whether the prospective business partner creates FCPA risk for the company. The due diligence should be tailored and as thorough as economically feasible. Moreover, even after the transaction has been finalized, MST companies should continue to maintain oversight of the Third Party to ensure continued compliance with the FCPA. The Third Party should be effectively integrated into the company's anti-corruption compliance protocols and training. Complete records and files relating to any due diligence performed on third parties should be maintained.

Insert FCPA Provisions in Third-Party Contracts. MST companies should include standard provisions in contracts with third parties that are reasonably calculated to prevent and detect FCPA violations. These provisions may, depending on the circumstances, include: (a) FCPA representations and undertakings relating to compliance with the FCPA; (b) the right to of the MST company to conduct audits of the books and records of the agent; and (c) termination rights if there is any breach of any anti-corruption law or a breach of representations and undertakings related to such matters, including the ability to disclaim and reverse any economic benefit that would otherwise be received based on the actions of the third parties.

Have a Procedure in Place for Dealing With Suspected Violations / Don't Ignore Red Flags. MST companies should have a system in place for reporting suspected violations of the FCPA compliance policies, standards, and procedures. Once such conduct is reported, the company must act quickly to (a) conduct a thorough internal investigation of the suspected violation; (b) stop any conduct determined to pose a risk to the company; and (c) impose appropriate discipline upon any offending party.

Conclusion

Because MST companies often do business with the U.S. government and foreign governments, a culture of legal compliance should be a fundamental component of their strategic approach to risk management. Between the increasing complexities of complying with statutes such as the FCPA and FCA, the more aggressive approach taken by U.S. enforcement agencies, and the global reach of such activity, strong and credible compliance practices are essential to reducing a MST company's risk of FCA or FCPA liability.

---

[i] *Vt. Agency of Natural Res. v. United States ex rel. Stevens*, 529 U.S. 765, 781 (2000), *citing United States v. Bornstein*, 423 U.S. 303, 309 (1976).

[ii] *See* H.R. Rep. No. 99-660, p.2 (1986) (stating that defense contractor fraud had increased by 30%)

[iii] *See Cook County, Ill. v. United States ex rel. Chandler*, 538 U.S. 119, 145 (2003) (quoting S. Rep. No. 99-345, p. 2 (1986)); *Minnesota Ass'n of Nurse Anesthetists v. Allina Health Sys. Corp*., 276 F.3d 1032, 1040-42 (8th Cir. 2002).

[iv] http://www.taf.org/statistics.htm

[v] In addition, although the American Recovery and Reinvestment Act, enacted in 2009, does not amend the FCA, it does offer further protection for potential relators. Under the Act, once an employee makes a formal or informal complaint to a supervisor or company representative regarding fraud, safety violations, public health issues, or illegal activity, the employee is granted whistleblower protection. Later, if the employee brings suit for retaliation, he or she only needs prove that the report resulted in harassment or discrimination. To rebut this, the employer must show by "clear

and convincing evidence" that the treatment had nothing to do with the whistleblower status.

[vi] *United States ex rel. Fine v. Chevron, U.S.A., Inc*., 72 F.3d 740, 742 (9th Cir. 1995).

[vii] *U.S. ex rel. King v. DSE, Inc., et al*., CV-2416-T-23EAJ (May 17, 2011).

[viii] *United States ex rel. Pogue v. Diabetes Treatment Ctrs. Of Am., Inc*., 238 F. Supp. 2d 258, 264 (D.D.C. 2002).

[ix] *See, e.g., U.S. ex rel. Bowan v. Education Am., Inc.*, No. 04-20384, 116 Fed. Appx. 531, 2004 WL 2712494 (5th Cir. Nov. 30, 2004).

[x] *See United States, et al., ex rel. Radcliffe v. Purdue Pharma L.P*., 2010 WL 1068229 (4th Cir. 2010). *See also United States ex rel. Whitten v. Triad Hospitals*, Inc., 2005 WL 3741538 *reversed on other grounds in Whitten v. Triad Hospital, Inc*., 210 Fed.Appx. 878 (11th Cir. 2006) (indicating that public policy favored enforcement of private contract in light of the fact that the Government chose not to intervene).

[xi] *See* DOJ press release, "Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme" (Jan. 19, 2010).

[xii] *See* 15 U.S.C. §§ 78dd-1 to -3 (2006).

[xiii] *See* DOJ press release, *supra* note 1.

[xiv] *Id.*

[xv] *See* 15 U.S.C. §§ 78dd-1 to -3, 78m(b)(2)(A) (2006).

[xvi] *See* 15 U.S.C. §§ 78dd-1 to -3 (2006).

[xvii] *Id.*

[xviii] *Id.*

[xix] Christopher Norton, *FBI Agent Details Undercover Role in Gabon FCPA Case*, Law360 (June 2, 2011), http://www.law360.com/whitecollar/articles/248903?utm_source=newsletter&utm_medium=email&utm_campaign=whitecollar.

[xx] *Id.*

[xxi] *Id.*

[xxii] *See* 15 U.S.C. § 78m(b)(2)(A) (2006).

[xxiii] Mike Koehler, *Foreign Corrupt Practice Act Enforcement in 2010: Big, Bold, and Bizarre*, 6 White Collar Crime Report 166, 167 (2011).

[xxiv] *Id.*

[xxv] *Id.*

[xxvi] SEC press release, *SEC Sues Former President of United Industrial Corporation Subsidiary for Authorizing the Payment of Foreign Bribes* (May 29, 2010).

[xxvii] Corrected Order Instituting Cease-And-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, *In re United Industrial Corp*. (May 29, 2009).

[xxviii] ACL's parent corporation was AAI Corporation, a direct, wholly owned subsidiary of UIC.

[xxix] Corrected Order, *supra* note 52.

[xxx] *Id.*

[xxxi] *Id.*

[xxxii] Complaint, *S.E.C. v. Wurzel*, 1:09-cv-01005 (D.D.C. May 29, 2009).

[xxxiii] Corrected Order, *supra* note 52.

[xxxiv] *Id*.

[xxxv] *Id*.

REFERENCES

Vt. Agency of Natural Res. v. United States ex rel. Stevens, 529 U.S. 765, 781 (2000), *citing United States v. Bornstein*, 423 U.S. 303, 309 (1976).

H.R. Rep. No. 99-660, p.2 (1986) (stating that defense contractor fraud had increased by 30%)

Cook County, Ill. v. United States ex rel. Chandler, 538 U.S. 119, 145 (2003) (quoting S. Rep. No. 99-345, p. 2 (1986)); *Minnesota Ass'n of Nurse Anesthetists v. Allina Health Sys. Corp*., 276 F.3d 1032, 1040-42 (8th Cir. 2002).

United States ex rel. Fine v. Chevron, U.S.A., Inc., 72 F.3d 740, 742 (9th Cir. 1995).

U.S. ex rel. King v. DSE, Inc., et al., CV-2416-T-23EAJ (May 17, 2011).

United States ex rel. Pogue v. Diabetes Treatment Ctrs. Of Am., Inc., 238 F. Supp. 2d 258, 264 (D.D.C. 2002).

U.S. ex rel. Bowan v. Education Am., Inc., No. 04-20384, 116 Fed. Appx. 531, 2004 WL 2712494 (5th Cir. Nov. 30, 2004).

United States, et al., ex rel. Radcliffe v. Purdue Pharma L.P., 2010 WL 1068229 (4th Cir. 2010).

United States ex rel. Whitten v. Triad Hospitals, Inc., 2005 WL 3741538 *reversed on other grounds in Whitten v. Triad Hospital, Inc*., 210 Fed.Appx. 878 (11th Cir. 2006)

Department of Justice Press Release (Jan. 19, 2010). "Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme"

15 U.S.C. §§ 78dd-1 to -3 (2006).

Christopher Norton (June 2, 2011), *FBI Agent Details Undercover Role in Gabon FCPA Case*, Law360 http://www.law360.com/whitecollar/articles/248903?utm_source=newsletter&utm_medium=email&utm_campaign=whitecollar.

Mike Koehler, *Foreign Corrupt Practice Act Enforcement in 2010: Big, Bold, and Bizarre*, 6 White Collar Crime Report 166, 167 (2011).

SEC Press Release (May 29, 2010), "SEC Sues Former President of United Industrial Corporation Subsidiary for Authorizing the Payment of Foreign Bribes"

Corrected Order Instituting Cease-And-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, *In re United Industrial Corp.* (May 29, 2009).

Complaint, *S.E.C. v. Wurzel*, 1:09-cv-01005 (D.D.C. May 29, 2009).