Bloomberg Law

Professional Perspective

FCPA Investigations, Trade Secrets, and Corporate Procurement Practices

Christine Streatfeild and Jane Klinger,
Baker McKenzie

FCPA Investigations, Trade Secrets, and Corporate Procurement Practices

Contributed by Christine Streatfeild and Jane Klinger, Baker McKenzie

Increased collaboration and information sharing between U.S. enforcement agencies and with foreign regulators have made companies more vulnerable than ever to an enforcement action that can implicate a number of criminal and civil statutes. Investigations under the U.S. Foreign Corrupt Practices Act often center on a company's procurement activities and interactions with third-party business partners.

Most companies understand that FCPA risks are high when using third parties to obtain government contracts—but the risk does not stop with the FCPA. What if your procurement team receives a friendly "tip" about a competitor's operations, such as its pricing, production capacity, or growth strategy in a region? What if a foreign official provides confidential bid information to your company that helps the company win the work?

These disclosures of another's sensitive business information may involve protectable trade secrets that expose your company to misappropriation claims—in addition to fraud, bid-rigging, and FCPA violations. In order to direct employees on how to properly identify, report, and respond to the disclosure of confidential business information, companies should incorporate policies and procedures for the treatment of trade secrets—both offensively and defensively—into their compliance programs.

Once an employee receives questionable information, whether solicited or not, it is critical that counsel effectively manage the situation. The employee may not know that he or she is now accessing a protectable trade secret that could subject the company to potential civil or criminal liability.

Growing Threat of Parallel Investigations

Trade secrets are a broad construct that include "financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, programmed devices, formulas … whether tangible or intangible." 18 U.S.C. §1839(3) (U.S. Defend Trade Secrets Act). As long as the information has independent economic value because it is not generally known or ascertainable and the owner has taken reasonable measures to keep it secret, then a wide range of business or technical information can qualify.

As companies expand the footprint of their operations and are increasingly decentralized, the risk of a breach of confidentiality or receipt of a third party's sensitive business information also grows. This matters because enforcement regimes have stepped up efforts in the past three years toward harmonizing certain aspects of trade secrets in critical jurisdictions.

For example, the U.S. passed the Defend Trade Secrets Act in 2016, the EU passed the Trade Secret Directive in 2016, and the People's Republic of China passed a bill amending the Anti-Unfair Competition Law in January 2018. The converging of components in trade secret regimes enhances predictability and provides consistency in terms of definitions, duties, and what constitutes misappropriation. It also exacerbates the risk of getting it wrong with the treatment of confidential information by broadening exposure.

The exposure is cross-border and, in the U.S., intersects with corruption investigations by the FBI, the Department of Justice, and the Securities and Exchange Commission. At the end of the 2018 fiscal year, the FBI had 195 pending intellectual property rights-based investigations. The largest number of investigations dealt with the theft of trade secrets (67), copyright infringement (64), and trademark infringement (64). The FBI initiated 54 new investigations, made 22 arrests, and obtained 12 convictions, forfeitures totaling $3,176,949, and restitutions totaling $64,549,217.

Companies face worldwide claims of unfair competition or misappropriation based on numerous acts by their employees or agents throughout their supply chain. The risk presents itself in several ways—including through the receipt of confidential information of another entity or through the loss of a company's trade secrets from a careless or rogue employee. When attempting to assert a company's own trade secret, the company will be required to show it met a standard of reasonable care in the protection of its information under the circumstances—which could increasingly be informed by industry norms, regardless of jurisdiction.

In the face of this exposure for actual or attempted trade secrets theft, companies must consider the impact of even one non-compliant employee or consultant, who may set up a criminal prosecution, civil lawsuit for the theft of trade secrets, or investigation.

Trade Secrets in the Procurement Function

Companies are quite comfortable with the trade secret protections afforded to things like a secret formula or a production process. Even so, in the case of a procurement department, companies may not understand how often their employees deal with trade secrets. Customer information, price lists, growth or development strategies, industry projections, and any other valuable and secret information about the business may also be a trade secret.

In many cases, an FCPA investigation that centers on the procurement team's activities and payments reveals that employees bribed or otherwise colluded to obtain sensitive pricing information or other details about their competitor's offerings. Often, it is clear that this information is subject to confidentiality agreements or other obligations not to disclose it, and that the information would be used to obtain an improper advantage in the bidding process. What's often not clear is that even if the company escapes FCPA liability, there could still be trade secret misappropriation risks that must be addressed.

What if the company receives the protected information about a competitor? What if an employee in a remote location of the world stumbles upon the sensitive business information of another party through otherwise routine discussions with third-party partners? A recipient of another's trade secrets may be liable for misappropriation—even if the information was not solicited—if the recipient knew or had reason to know that the disclosing party was under an obligation to keep the information confidential. See *AccentCare Home Health of Rogue Valley LLC v. Bliss*, 2017 U.S. Dist. LEXIS 88125 (D. Or. April 13, 2017) ("the acquirer of the trade secrets can be sued separately from the person who disclosed them, if the acquirer knew or should have known that the secrets were improperly acquired").

In a recent U.S. case, for example, a coil manufacturer faced trade secret allegations where circumstantial evidence showed that it had a pattern of receiving a competitor's drawings through customers. *Bal Seal Eng'g v. Nelson Products*. The court allowed the trade secret claim to proceed to trial after reviewing email chains between the manufacturer and its customers where the customers requested quotes based on the competitor's drawings and part numbers.

Holistic, Risk-Based Corporate Compliance Program

Companies should take a holistic, risk-based approach to address exposure in the (mis)treatment of confidential information. Issues associated with the FCPA are legally distinct from trade secrets, and most employees trained on anti-bribery and corruption are not thinking about trade secrets as a potential risk area. This is because the common assumption is that another function focused on intellectual property is managing this risk. However, in practice, there is meaningful overlap in terms of exposure points, compliance activities, and opportunities to reduce risks of loss or investigation. Both issues are regulated by the DOJ and SEC, and can arise from fraud, collusion and bid-rigging in the procurement process.

A trade secret is considered something 'of value' for purposes of the FCPA and can therefore attach liability if provided corruptly to a foreign official. Integrating a trade secrets component into the company's compliance materials and training activities ensures information-sharing and input from stakeholders across the legal, compliance, procurement, finance, and intellectual property functions. Moreover, effective corporate compliance programs provide both a defense to allegations of wrongful conduct and an affirmative showing of 'reasonable measures' to secure company secrets.

The DOJ recently updated its Guidance on Evaluation Corporate Compliance Programs to enable companies to understand the Department's current thinking on best practices in corporate program design and implementation. As Assistant Attorney General Brian Benczkowski noted in his remarks announcing the publication of the Guidance on April 30, 2019, there are three significant decisions made by the Department in resolving a corporate criminal matter that will involve an analysis of the company's compliance program by prosecutors:

Charging Decision. "First, pursuant to the Justice Manual, prosecutors assess the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision. This helps guide the prosecutors in determining whether they should decline to bring a case, or, if a resolution is appropriate, what that resolution should be."

Sentencing Decision. "Second, prosecutors assess a company's compliance program at the time of the misconduct to determine the company's culpability score under the U.S. Sentencing Guidelines, which determines the company's ultimate fine range."

Imposition of Compliance Monitor. "Third, prosecutors look at the company's compliance program at the time of the resolution to determine whether an independent compliance monitor is necessary to prevent the reoccurrence of misconduct, or whether the compliance program is sufficiently effective to permit the company to self-monitor."

Most importantly, the updated guidance serves as a timely reminder of DOJ's evaluation priorities, and its continued focus on effective corporate compliance programs as the keystone to the prevention, detection and remediation of corporate wrongdoing.