Recent Federal Prosecution Highlights Risks of Receiving Competitors' Confidential Information From a Customer

Skadden

November 12, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorney or call your regular Skadden contact.

James J. Fredricks
Partner / Washington, D.C.
202.371.7140
james.fredricks@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

On September 30, 2024, the DOJ announced that Siemens Energy, Inc., pleaded guilty to a federal fraud charge and agreed to pay a $104 million fine for rigging a bid by using rivals' bidding information wrongfully obtained from one of the customer's employees.

The prosecution sends a cautionary message about the circumstances in which obtaining market intelligence crosses the line to illicit misappropriation of confidential information. It reminds companies that manipulating a bidding process, even without a traditional bid-rigging agreement among the bidders, can yield criminal charges and substantial fines.

United States v. Siemens Energy, Inc.

According to the federal charge, Dominion Energy, Inc., a utility company based in Richmond, Virginia, conducted a closed-bid process to purchase equipment and related long-term service agreements for a new gas turbine plant. It solicited proposals from Siemens Energy, General Electric Company (GE), and Mitsubishi Heavy Industries, Ltd. (MHI), entering bilateral non-disclosure agreements with each of them as part of the process. These agreements limited the use and disclosure of confidential and proprietary information shared as part of the bid process, including pricing for units and optional features.

After the bids were submitted, a Siemens account manager called a Dominion manager to inquire into "'the numbers' of GE's and MHI's bids" to "ascertain whether Siemens' bid had been competitive." The manager explained he did not have access to the confidential information, but could obtain it. In a later phone call, the Dominion manager relayed to the Siemens account manager the top line bid amounts of the two other bidders.

Subsequently, the two managers worked to "funnel GE and MHI Confidential Information" to Siemens. That information included details on unit pricing and optional features, and on at least one occasion, a competitor's revised bid marked "Proprietary & Confidential Information."

The managers used personal email accounts, for example, sending documents from a Dominion email address to a Google email address, and then to a spouse's Hotmail email account, and then to a Yahoo email address, and finally to a Siemens email address. The Siemens account manager forwarded the GE and MHI confidential information to a Siemens regional manager, who passed it on to a Siemens executive vice president. The executive vice president shared some of the confidential information with leaders in Siemens' business intelligence unit.

Knowing or remaining "willfully blind" to the fact Siemens was not entitled to the GE and MHI confidential information, the company used it to gain a competitive advantage in the Dominion bidding and future bids against GE and MHI, including using it to submit a lower bid and undercut GE's bid for the Dominion project.

The DOJ charged Siemens with a wire fraud conspiracy. By "illicitly obtaining GE and MHI confidential information," the company intended to "unlawfully enrich Siemens, to the economic detriment of GE and MHI," and to "obtain an unfair competitive advantage."

In its plea agreement, Siemens agreed that a statutory provision increasing the maximum fine to twice the gross gain or loss from the offense authorized the agreed-upon $104 million fine. The Siemens account manager, regional manager, and executive vice president and the Dominion manager separately pleaded guilty for their roles in the scheme and received prison sentences ranging from 21 to 43 months.

Recent Federal Prosecution Highlights Risks of Receiving Competitors' Confidential Information From a Customer

Bid-Rigging Charges Without an Agreement Among Competitors

The cornerstone of most antitrust corporate compliances programs is policing the giving or receiving of sensitive competitive information, such as price or bid amounts, to or from competitors. The risks associated with that kind of sharing are well understood and significant — potentially Sherman Antitrust Act charges for conspiring with competitors to rig bids or fix prices, prison sentences for culpable executives, and criminal fines and treble damages awards against the company.

Less appreciated are the risks when a customer provides sensitive information about a competitor. While a bid-rigging charge under the Sherman Antitrust Act requires a competitor-to-competitor agreement, the Antitrust Division and other DOJ components have a history of charging defendants under other statutes when they wrongfully obtain confidential information from agents or employees of the customer to manipulate bidding.

For example, in a series of cases in the 2010s, the Antitrust Division charged financial institution employees who were bidding to provide investment contracts to municipalities with fraud for, in the Second Circuit's words, paying "kickbacks" to the municipalities' brokers to tell "what others were bidding, which allowed the Defendant to lower an initial bid if it significantly exceeded the second-place bid, or to raise the bid to a level just high enough to win the contract." *United States v. Grimm*, 738 F.3d 498, 500 (2d Cir. 2013).

More recently, the Antitrust Division obtained a guilty verdict against an employee at the federal Strategic Petroleum Reserve, who provided confidential information to a company to give it a competitive advantage on its bids for work at the reserve, for conspiracy to defraud and to violate the Procurement Integrity Act. The government also obtained a guilty plea by the company.

Unlike the sharing of bids and prices among competitors, which is generally avoided, it is not unusual for customers to share information about competitors. During negotiations, for example, a customer may share a competitor's price or discount to persuade another competitor to improve its offer. Or a customer may laud a competitor's anticipated quality or feature improvements to spur improvements or concessions by another competitor. The key difference lies between legitimately receiving information enabling greater (albeit fair) competition and wrongfully misappropriating or obtaining information to manipulate the competition.

In the Siemens case, the government's allegations included a number of *indicia* supporting its charge that the conduct was undertaken with a fraudulent or wrongful intent:

- The bilateral nondisclosure agreement between Siemens and Dominion put Siemens on notice of what bidding information was confidential and that its disclosure would violate the others' nondisclosure agreements.
- The Siemens account manager solicited the information from a Dominion manager, who initially responded that he did not have access to the confidential information. It was not a case of a Dominion agent entitled to the information using it unsolicited in the normal course of a negotiation.
- Siemens received competitors' documents, including a revised bid marked "Proprietary & Confidential Information."
- The Siemens account manager and Dominion manager funneled the information through a series of personal email accounts, rather than through normal business communication channels emails.

Risk Mitigation: Do's and Don'ts

While a bright line rule against receiving competitor information from customers (unlike a general rule against sharing prices with competitors) is likely unworkable, there are steps companies can consider taking consistent with risk mitigation and business practices. These steps should not be mistaken for legal requirements, nor does their absence indicate wrongdoing, let alone amount to a violation of law. Rather, they reflect insights on ways to reduce risk.

Businesses can limit the receipt to information customarily shared in negotiations and avoid receipt of a large, detailed, extraneous or continuous stream of competitor information. They can use the information to improve its competitive position and consult counsel whenever there are signs that might suggest improperly derived information.

- **Do** know and document the source of sensitive or competitive information or intelligence.
- **Do** keep communications with customers on regular, official business channels.
- **Do** internally disseminate only information relevant to improving competitive posture.
- **Do** negotiate and compete vigorously and in good faith.
- **Do** consult counsel when information indicates that it was improperly derived.
- **Do not** accept competitive intelligence from competitor's employees or agents.

Recent Federal Prosecution Highlights Risks of Receiving Competitors' Confidential Information From a Customer

- **Do not** solicit customers for competitively sensitive information about a competitor.
- **Do not** provide a "kickback" or reward in any form to a customer in return for such information.
- **Do not** internally disseminate information without consulting counsel if there are *indicia* that the information was improperly obtained.
- **Do not** use information from a customer for anticompetitive purposes, such as aligning on prices with competitors.