wiley

NEWSLETTER

When an Employee Takes Proprietary Materials

November 2016

Government Contracts Issue Update

The risk that a current or departing employee will misappropriate proprietary company information is ever-present for government contractors. A government contractor employee might take company documents or data for any number of reasons. For instance, the employee could be planning to use the materials to gain a competitive advantage at the next job, or to sue the company for employment-related claims. An employee who believes the documents show fraud or other illegalities might hope to bring justice to a perceived wrong (or, perhaps more selfishly, for a big payday or publicity as a whistleblower).

To protect the company's proprietary information and legal rights, every government contractor should have a specific response plan for when it believes an employee has improperly taken company documents. This article provides concrete steps and important considerations for reacting to theft of proprietary materials, including a new federal law that empowers employers to take immediate action in federal court when proprietary information is stolen.

Investigate immediately

The first step when an employee may have taken documents is to conduct an immediate investigation directed by counsel. The company should lock down the employee's computer, devices, and accounts in order to prevent further misappropriation of documents and preserve the electronic record. The company should then begin a forensic investigation to assess the scope of the employee's misappropriation: what documents were taken, how were they

Authors

Mark B. Sweet
Partner
202.719.4649
msweet@wiley.law

Practice Areas

Government Contracts

accessed, what was done with them, and how can any gaps in data security protocols be closed to prevent further data exfiltration? If the activity involves a current employee, it may be necessary to place the employee on administrative leave pending the outcome of the investigation and any decisions on continued employment.

The company should also interview people who worked with the employee in order to understand potential motive and the risk of potential wrongdoing—for instance, whether the employee may be acting as a whistleblower based on previous expression of concerns of discrimination, fraud, or other potentially illegal conduct. The entire investigation should be directed by counsel to preserve confidentiality and privilege, ensure thoroughness, and lend credibility to the investigation in the event it becomes relevant in a subsequent government disclosure, investigation, or lawsuit.

Assess the legal implications and options

Once the company has a sense of what materials were taken, it should assess the legal significance of the materials and the company's legal options and obligations. Theft of trade secrets may provide grounds and good reason for immediate legal action. Under the Defend Trade Secrets Act (DTSA), which became federal law in May, a victim of trade secrets theft can file suit in federal district court and seek a number of remedies, including injunctive relief to prevent actual or threatened misappropriation, *ex parte* seizure of property to prevent the disclosure or dissemination of trade secrets, and money damages (including double damages and attorney's fees in some circumstances). Most states provide similar remedies under state law. If the theft occurred electronically, the Computer Fraud and Abuse Act may be a basis for a civil suit. The company may also have grounds to sue the individual for tort claims.

The company should also analyze any employment or non-disclosure agreements signed by the employee. These agreements may include liquidated damages or a right to seek attorney's fees if the company prevails in litigation. Short of litigation, the company can send a letter notifying a former employee of the grounds for liability and demanding immediate return of the materials. If it appears the former employee plans to use the company's proprietary information in employment with a competitor, the company should consider notifying the competitor as well.

If the company wants to be aggressive without necessarily taking on the full burden of civil litigation, it can refer the matter to law enforcement for a potential criminal prosecution. Indeed, notifying law enforcement may be required by federal and state regulations in some situations, such as when classified information, personal information, or health information has been misappropriated. If the stolen information belongs to or reveals confidences of a customer, notifying customers may be necessary as well.

The company may have other options if it learns about the misappropriation while the person is still employed with the company. The company's code of conduct and other policies likely spell out that misuse or disclosure of confidential company information is grounds for discipline, even termination.

While aggressive action is often justified and necessary to protect the company, the company may want to proceed more cautiously if the Government is involved or could become involved. Under the terms of its

contract or the Federal Acquisition Regulation, the government may own the intellectual property that has been stolen, which may limit the company's ability to claim a trade secret. Additionally, federal and state laws provide whistleblower protections that will require careful consideration. For example, the DTSA immunizes individuals from liability for confidentially disclosing trade secrets to government officials or to attorneys for the purpose of reporting or investigating suspected legal violations. Other statutes, such as the False Claims Act and Sarbanes-Oxley, prohibit retaliatory adverse employment actions against current employees who are engaging in protected activity. To the extent there might be a government investigation related to the company documents, aggressive action against the employee (whether current or former) could be viewed by the Government as an attempt to muzzle a whistleblower. In fact, if the company believes that the employee plans to share the information with the Government, the best response may be a proactive disclosure to the inspector general, contracting officer, or suspension and debarment official that provides appropriate context and puts the company in the best light possible.

In short, the company should assess all of its legal options while keeping in mind the potential consequences of going after a purported whistleblower—especially when viewed through the eyes of a government investigator. If aggressive action is still warranted, make sure to document the reasons and justifications for each step and consider briefing potential stakeholders before the theft or the company's response becomes public knowledge.

Strengthen compliance, training, and data security

Finally, an employee's misappropriation of company materials should be treated as an opportunity to learn about vulnerabilities and to prevent recurrences. Potential whistleblowers often take company materials as a way of taking matters into their own hands because they voiced concerns but believe they were not heard. If this is the case—and regardless of whether the employee's concerns have merit—the company should consider strengthening its internal reporting channels and re-training employees on how to use them. The company should review its policies to make sure the definition of proprietary materials is clear and the policy is communicated routinely. Employees should be reminded of the potentially severe legal consequences of misappropriating trade secrets and other proprietary information. Finally, the company should assess whether the breach exposed vulnerabilities in data security that should be addressed.

For more information, please contact a Wiley Rein attorney.