Is Theft of Trade Secrets a Crime Under Federal Law?

Devin Bates
dbates@mwlaw.com
(501) 688.8864

10/23/2024

Is Theft of Trade Secrets a Crime Under Federal Law? Yes. In this installment, we'll focus on the Economic Espionage Act (EEA) and the Defend Trade Secrets Act (DTSA), as well as the Computer Fraud and Abuse Act (CFAA). Theft of trade secrets is also a crime under state law.

Economic Espionage Act (EEA) and Defend Trade Secrets Act (DTSA)

Before the Defend Trade Secrets Act (DTSA) was enacted in May 2016, the Economic Espionage Act (EEA) provided criminal penalties for trade secret theft but did not allow for civil claims by employers. Today, the EEA still establishes criminal penalties, while the DTSA provides avenues for civil remedies.

The EEA defines two primary types of criminal conduct involving trade secrets:

- **Trade Secret Theft:** Unlawful acquisition, use, or disclosure of trade secrets.
- **Foreign Economic Espionage:** Trade secret violations intended to benefit a foreign government or entity sponsored by a foreign government.

The penalties applicable in each case can vary. But in general, the penalties available under the EEA include the following.

For trade secret theft:

- Individuals may face fines, up to ten years in prison, or both.
- Organizations may be fined up to $5 million or three times the value of the stolen trade secret, including expenses avoided.

For foreign economic espionage:

- Individuals may be fined up to $5 million, face up to 15 years in prison, or both.
- Organizations may be fined up to $10 million or three times the value of the stolen trade secret, including expenses avoided.

Computer Fraud and Abuse Act (CFAA)

The CFAA provides another layer of protection against trade secret theft through criminal penalties for unauthorized computer access. The CFAA allows for civil actions by any person who suffers damage or loss due to a violation. Unlike the EEA and DTSA, the CFAA does not require that the accessed data be a trade secret—only that it is valuable to the owner.

Historically, there was a divide among courts regarding whether the CFAA could be used against employees who had authorized access to a computer but used that access to obtain or alter information beyond the scope of their authorization. Some courts adopted a narrow interpretation, focusing strictly on unauthorized access, while others took a broader view, considering unauthorized use.

However, the Supreme Court resolved this split in authority in its decision Van Buren v. U.S., 141 S. Ct. 1648 (2021), therein adopting the narrow approach. The Court held that the CFAA does not cover individuals who have authorized access but use the information improperly.

Impact of the DTSA and Supreme Court Ruling on CFAA Claims

Employers traditionally used the CFAA to bring trade secret disputes into federal court. However, with the DTSA providing direct access to federal courts for trade secret misappropriation claims, and the Supreme Court's narrow interpretation of unauthorized access under the CFAA, the appeal of using the CFAA in trade secret disputes has softened.

Conclusion

Trade secret theft can indeed be a crime under federal law, particularly under the Economic Espionage Act and the Computer Fraud and Abuse Act. The DTSA adds civil remedies, providing a robust framework for businesses to protect their trade secrets. As the legal landscape evolves, understanding the implications of these laws is crucial for businesses looking to safeguard their confidential information.

This content was prepared for publication with the assistance of ChatGPT.