Congressional Research Service
Informing the legislative debate since 1914

Stealing Trade Secrets and Economic Espionage: An Abridged Overview of the Economic Espionage Act

Updated October 29, 2024

Congressional Research Service
https://crsreports.congress.gov
R42682

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Stealing a trade secret is a federal crime when the information relates to a product in interstate or foreign commerce, 18 U.S.C. § 1832 (theft of trade secrets), or when the intended beneficiary is a foreign power, 18 U.S.C. § 1831 (economic espionage). Section 1832 requires that the thief be aware that the misappropriation will injure the secret's owner to the benefit of someone else. Section 1831 requires only that the thief intend to benefit a foreign government or one of its instrumentalities.

Offenders face lengthy prison terms as well as heavy fines, and they must pay restitution. Moreover, property derived from the offense or used to facilitate its commission is subject to confiscation. The sections reach violations occurring overseas if the offender is a United States national or if an act in furtherance of the crime is committed within the United States.

Depending on the circumstances, misconduct captured in the two sections may be prosecuted under other federal statutes as well. A defendant charged with stealing trade secrets is often indictable under the Computer Fraud and Abuse Act, the National Stolen Property Act, or the federal wire fraud statute. One indicted on economic espionage charges may often be charged with acting as an unregistered foreign agent and on occasion with disclosing classified information or under the general espionage statutes. Finally, by virtue of the Defend Trade Secrets Act (P.L. 114-153), §§ 1831 and 1832 are predicate offenses for purposes of the federal racketeering and money laundering statutes.

The Defend Trade Secrets Act dramatically increased EEA civil enforcement options when it authorized private causes of action for the victims of trade secret misappropriation. In addition, the EEA now permits pre-trial seizure orders in some circumstances, counterbalanced with sanctions for erroneous seizures.

This report is an abridged version, without the footnotes or attribution for quotations found in the parent version, of CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*.

Contents

Contacts

Introduction[1]

The Economic Espionage Act (EEA) outlaws two forms of trade secret theft: theft for the benefit of a foreign entity (economic espionage) and theft for pecuniary gain (theft of trade secrets). Under either proscription, the EEA's reach extends to theft from electronic storage. Individual offenders face imprisonment for up to 15 years for economic espionage and up to 10 years for trade secret theft. Individuals also may incur fines of up to $250,000 or twice the loss or gain associated with the offense for trade secret theft, whichever is greater. For economic espionage, individuals face fines of up $5 million or twice the loss or gain. Organizations are fined more severely. They can be fined up $5 million, twice the loss or gain associated with the offense, or three times the value of the stolen trade secret, for trade secret theft. For economic espionage, the fines for organizations jump to a maximum of the greater of $10 million, three times the value of the trade secret, or twice the gain or loss associated with the offense.

A court may assess the same sanctions for attempt or conspiracy to commit either offense, or for aiding or abetting the completed commission of the either offense. A sentencing court must order the defendants to pay victim restitution, and the government may confiscate any property that is derived from or used to facilitate either offense. The government may seek to enjoin violations, and, by virtue of amendments in the Defend Trade Secrets Act of 2016, victims may be entitled to sue for double damages, equitable relief, and attorneys' fees.

Conduct that violates the EEA's proscriptions may also violate other federal prohibitions. Some statutes, like the Computer Fraud and Abuse Act, impose criminal penalties and also authorize victims to sue for damages and other forms of relief under some circumstances.

Stealing Trade Secrets

The trade secrets prohibition is the more complicated of the EAA's two criminal offenses. It condemns:

- Whoever
- with intent to convert
- a trade secret
- related to a product or service used in or intended for use in interstate commerce or foreign commerce
- to the economic benefit of anyone other than the owner thereof
- intending or knowing that the offense will injure the owner of that trade secret
- knowingly steals, without authorization appropriates, takes, carries away, conceals, or by fraud, artifice, or deception obtains such information, [or] without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; [or] receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

or

- Whoever attempts or conspires [to do so].

[1] This report is an abridged version, without the footnotes or attribution for quotations found in the parent reversion, of CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, by Charles Doyle.

Whoever: The term "whoever" encompasses both individuals and organizations. Thus, individuals and organizations may be guilty of the theft of trade secrets. Subsection 1832(b) confirms this intent by establishing a special fine for "organizations" who commit the offense. For purposes of the federal criminal code, an "organization" is any "person other than an individual." The Dictionary Act supplies examples of the type of entities that may qualify as "persons," i.e., "the words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals."

With Intent to Convert: Conversion is a common law concept which is defined as "[t]he wrongful possession or disposition of another's property as if it were one's own" or "an act or series of acts of willful interference, without lawful justification, with any item of property in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the property." This "intent to steal" element, coupled with the subsequent knowledge and "intent to injure" elements, would seem to ensure that a person will not be convicted of theft for the mere inadvertent or otherwise innocent acquisition of a trade secret.

A Trade Secret: An EEA trade secret is any information that "(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." An owner for these purposes is one "in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed." Whether an owner has taken reasonable measures to ensure the secrecy of his trade information will depend upon the circumstances of the case. Such measures would ordinarily include limiting access to the information and notifying employees of its confidential nature. Inclusion within the definition of "trade secret" of the instruction that the owner take "reasonable measures" to secure the confidentiality of the information does not render the statute unconstitutionally vague as applied to a defendant whose conduct clearly falls within the statute's proscription.

Construction of the "known or readily ascertainable" element of the secrecy definition is more perplexing. On its face, the EEA suggests that information is secret if it is unknown or undiscoverable by the general public, even if it might be known or discoverable within the industry in which the information is relevant. Congress, however, may have intended a narrower interpretation of "secret," that is, the information is secret only if it is not known to or reasonably ascertainable either by the general public or within the industry in which the information has value.

The EEA's definition of "trade secret" is "based largely on the definition of that term in the Uniform Trade Secrets Act." The EEA definition initially referred to information known to or readily ascertainable by the "public." The Uniform Trade Secrets Act (UTSA) definition, however, refers not to the public but to information known to or readily ascertainable by "other persons who can obtain economic value from its disclosure or use." The Defend Trade Secrets Act replaced the original definition with the UTSA language.

Product in Commerce: The trade secret must have an interstate or foreign commerce nexus. More specifically, it must be one "that is related to a product or service used in or intended for use in" such commerce. Congress settled upon this phrase after an appellate court held that earlier language covered only theft of a trade secret related to a product that was, or was intended to be, sold or otherwise placed in the stream of commerce.

Economic Benefit of Another: Someone other than the trade secret's owner must be the intended beneficiary of the theft or destruction. The thief may be, but need not be, the intended beneficiary. Moreover, a close reading of the statute argues for the proposition that no economic benefit need

actually accrue; economic benefit need only be intended. Yet if no economic benefit is intended, there is no violation.

Intent to Injure: The government must prove that the defendant intended to injure the trade secret's owner or that he knew the owner would be injured. However, it need not show actual injury. The section "does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." Again, the element addresses the defendant's state of mind, not reality. Nothing in the statute's language demands that the government prove actual injury.

Knowingly: The last of the section's three mens rea requirements demands that the defendant be aware that he is stealing, downloading, or receiving a stolen trade secret. There is some dispute over whether this requires the prosecution to prove that the defendant knew that he was stealing, downloading, or receiving *proprietary information* or that he knew that he was stealing, downloading, or receiving a *trade secret*. The Department of Justice has used the section's legislative history to reinforce its understanding of this feature of the section.

The courts have not always agreed. Some insist that the prosecution show that the defendant knew the information "had the general attributes of a trade secret."

Stealing and the Like: A person may be guilty of the theft of a trade secret only if he "knowingly" steals a trade secret, replicates a trade secret, destroys or alters a trade secret, or receives a stolen trade secret. Each of the alternative means of deprivation is cast in a separate subsection. The first subsection covers not only stealing a trade secret, but also concealing it or acquiring it by fraud.

Trade secrets are information and thus can be simultaneously held by an owner and a thief. As a result, the second subsection covers situations where the owner is not necessarily deprived of the information, but is denied control over access to it. It proscribes unauthorized copying, downloading, uploading, or otherwise conveying the information. It also outlaws alteration or destruction of a trade secret. The Justice Department has argued that this second means of misappropriation includes instances where a faithless employee, former employee, or cyber intruder commits the trade secret to memory and subsequently acts in a manner necessary to satisfy the other elements of the offense. It makes the point with some caveats, however:

> This is not to say, however, that any piece of business information that can be memorized is a trade secret. As noted, the EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill, or abilities. When the actions of a former employee are unclear and evidence of theft has not been discovered, it may be advisable for a company to pursue its civil remedies and make another criminal referral if additional evidence of theft is developed. Where available, tangible evidence of theft or copying is helpful in all cases to overcome the potential problem of prosecuting the defendant's "mental recollections" and a defense that "great minds think alike."

The third subsection outlaws the knowing receipt of stolen trade secret information. Conviction requires proof that a trade secret was stolen or converted in violation of one of the other subsections and that the defendant knew it.

Attempt and Conspiracy: Defendants who attempt to steal a trade secret face the same penalties as those who succeed. Attempt consists of intent to commit the offense and a substantial step toward the attainment of that goal. This would indicate that the information which the defendant seeks to steal need not be a trade secret, as long as he believes it is. Defendants who conspire to steal a trade secret also face the same penalties as those who commit the substantive offense. "In order to find a defendant guilty of conspiracy, the prosecution must prove . . . that the defendant possessed both the intent to agree and the intent to commit the substantive offense. In addition, the government must prove that at least one conspirator committed an overt act, that is, took an

affirmative step toward achieving the conspiracy's purpose." It is no defense that circumstances, unbeknownst to conspirators, render success of the scheme unattainable, as for example when the defendants plotted to steal information that was not in fact a trade secret.

Consequences: Individual offenders face imprisonment for up to 10 years and fines of up to $250,000. The court may fine an organization up to $5 million upon conviction. Individuals face a higher maximum fine if twice the gain or loss associated with the offense exceeds the statutory maximum (i.e., $250,000). The corresponding increase for organizations is the greater of the statutory amount ($5,000,000) or three times the gain realized by the defendant. A sentencing court must also order the defendant to pay restitution to the victims of the offense. Property derived from, or used to facilitate, commission of the offense may be subject to confiscation under either civil or criminal forfeiture procedures. The Attorney General may sue for injunctive relief, and owners may sue for damages, equitable relief, and attorneys' fees. Finally, the offense is a predicate offense under the Racketeer Influenced and Corrupt Organizations Act (RICO) and consequently a money laundering predicate offense.

Economic Espionage

The EEA's economic espionage and theft of trade secret offenses share many of the same elements. There are four principal differences. The theft of a trade secret must involve the intent to benefit someone other than the owner. It must involve an intent to injure the owner. And, it must involve a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce." Economic espionage, on the other hand, must involve an intent to benefit a foreign entity or at least involve the knowledge that the offense will have that result. It does not require an intent to injure the owner. And, it applies to any trade secret, notwithstanding the absence of any connection to interstate or foreign commerce. Finally, economic espionage is punished more severely. The maximum term of imprisonment is 15 years rather than 10 years, and the maximum fine for individuals is $5 million rather than $250,000. For organizations, the maximum fine is the greater of $10 million or three times the value of the trade secret rather than $5 million. As in the case of stealing trade secrets, the maximum permissible fine may be higher if twice the amount of the gain or loss associated with the offense exceeds the otherwise applicable statutory maximum. And the crime is likewise a RICO and, consequently, a money laundering predicate offense.

Section 1831 condemns:

- Whoever
- intending or knowing the offense will benefit
- a foreign government, a foreign instrumentality, or a foreign agent
- knowingly
- steals, without authorization appropriates, takes, carries away, conceals, or by fraud, artifice, or deception obtains a trade secret, [or] without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; [or] receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

or

- Whoever
- attempts [or] conspires [to do so].

Foreign Beneficiary: A casual reader might conclude that any foreign entity would satisfy Section 1831's foreign beneficiary element. Section 1839's definition of foreign agent and foreign

instrumentality, however, makes it clear that an entity can only qualify if it has a substantial connection to a foreign government. The definition of foreign instrumentality refers to foreign governmental control or domination. The description of a foreign agent leaves no doubt that the individual or entity must be the agent of a foreign government.

The theft of a trade secret demands an intent to confer an economic benefit. Economic espionage is not so confined. Here, "benefit means not only economic benefit but also reputational, strategic, or tactical benefit." Moreover, unlike the theft offense, economic espionage may occur whether the defendant intends the benefit or is merely aware that it will follow as a consequence of his action. As in the case of trade secret theft, however, the benefit need not be realized; it is enough that defendant intended to confer it.

Common Procedural Matters

Protective Orders: It would be self-defeating to disclose a victim's trade secrets in the course of the prosecution of a thief. Consequently, the EEA authorizes the trial court to issue orders to protect the confidentiality of trade secrets during the course of a prosecution and permits the government to appeal its failure to do so. The government may not appeal an order to reveal information it has already disclosed to the defendant. Nevertheless, in such instances, appellate review of a district court's disclosure order may be available through a writ of mandamus.

Extraterritoriality: The Supreme Court has said on a number of occasions that "[i]t is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'" With this in mind, Congress specifically identified the circumstances under which it intended the economic espionage and theft of trade secrets provisions to apply overseas. Either offense may be prosecuted as long as the offender is a U.S. national or an act in furtherance of the offense is committed within this country.

The legislative history indicates that these are the only circumstances under which violations abroad may be prosecuted. This may mean that foreign conspirators may not be charged unless some overt act in furtherance of the scheme occurs in the United States.

Prosecutorial Discretion: For five years after passage of the EEA, neither economic espionage nor trade secret violations of its provisions could be prosecuted without the approval of senior Justice Department officials. Prosecutors must still secure approval before bringing charges of economic espionage, but approval is no longer necessary for the prosecution of theft of trade secret charges.

Civil Remedies

For some time, the EEA authorized the Attorney General to bring a civil action to enjoin violations of its provisions, but it did not authorize a corresponding private cause of action. The Defend Trade Secrets Act created a private cause of action.

Private Cause of Action: The EEA now provides that "[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." Not just anyone who suffers damage as the result of trade secret misappropriation; only "owners" may sue. EEA, however, defines the term "owners" to include licensees. The trade secrets protected by civil suit are the same as those protected by the criminal proscriptions. The definition of the action that gives rise to liability—"misappropriation"—is taken from the UTSA. The term

encompasses acquiring, disclosing, or using a trade secret taken from its owner by scurrilous ("improper") means.

Pre-trial Seizure: Perhaps the EEA's most distinctive feature is its pre-trial seizure procedure. It allows an owner who alleges that his trade secret has been appropriated to apply to the court for an ex parte order seizing the purported trade secret. The procedure is replete with restrictions on its use, some reminiscent of the limitations on a temporary restraining order (TRO) in federal civil actions: inadequacy of alternatives; a threat of immediate and irreparable harm; a likelihood of success on the merits; and a favorable balance of harms. Yet, the procedure is confined to instances where a TRO is insufficient. "The ex parte seizure provision is expected to be used in instances in which a defendant is seeking to flee the country or planning to disclose the trade secret to a third party immediately or is otherwise not amendable to the enforcement of the court's orders."

The party from whom the trade secret is seized is entitled to a hearing within seven days, at which the owner of the trade secret bears the burden justifying the seizure order. Anyone injured by a "wrongful or excessive" seizure may sue for the relief described in the Trademark Act; that is, for "damages for lost profits, cost of materials, loss of good will, and punitive damages in instances where the seizure was sought in bad faith, and, unless the court finds extenuating circumstances, to recover a reasonable attorney's fee."

Damages and Equitable Relief: Relying heavily on the UTSA, EEA empowers district courts to award an aggrieved owner equitable relief; damages; and in the case of willful and malicious misappropriation, double damages and attorneys' fees. The court may also award attorneys' fees to a party who prevails against a bad faith claim of misappropriation. Equitable relief may also include a preliminary injunction where the movant has shown (1) a likelihood of success on the merits, (2) a likelihood of irreparable harm to the movant absent an injunction, (3) the balance of equities tips in the movant's favor, and (4) an injunction is in the public interest.

An action for the misappropriation must be brought within three years of when it is discovered or would have been discovered with the exercise of reasonable diligence, although the contracting parties may agree to a shorter period for filing claims.

Like criminal misappropriation prosecutions, civil misappropriation actions are subject to extraterritoriality provisions.

Author Information

Charles Doyle
Senior Specialist in American Public Law

Disclaimer