Congressional Research Service
Informing the legislative debate since 1914

# Stealing Trade Secrets and Economic Espionage: An Abridged Overview of 18 U.S.C. 1831 and 1832

**Charles Doyle**
Senior Specialist in American Public Law

July 25, 2014

**Congressional Research Service**
7-5700
www.crs.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.

Section 1832 (theft) violations are punishable by imprisonment for not more than 10 years, or a fine of not more than $250,000 (not more than $5 million for organizations), or both. Section 1831 (espionage) violations by individuals are punishable by imprisonment for not more than 15 years, or a fine of the greater of not more than $5 million, or both. Section 1831 violations by organizations are punishable by a fine of not more than the greater of $10 million or three times the value of the stolen trade secret. Maximum fines for both individuals and organizations may be higher when the amount of the gain or loss associated with the offense is substantial. Any attempt or conspiracy to commit either offense carries the same penalties as the underlying crime. Offenders must also be ordered to 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, and/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.

P.L. 112-269 set the maximum fines described above. It also instructed the United States Sentencing Commission to examine the sufficiency of federal sentencing guidelines and policies in the area of stealing trade secrets and economic espionage. P.L. 112-236 amended the trade secrets prohibition of 18 U.S.C. 1832 to overcome the implications of the Court of Appeals' *Aleynikov* decision. That decision held that the section did not outlaw the theft of computer code designed to facilitate a company's commercial transactions, because the code did not relate to a product to be placed in the stream of commerce.

This report is an abridged version, without the footnotes or attribution found in the longer report, CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832*.

# Contents



## Contacts

# Introduction

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, its reach extends to theft from electronic storage. Offenders face imprisonment for not more than 10 years in the case of trade secret theft and not more than 15 years in the case of economic espionage. Individuals may incur fines of not more than the greater of $250,000 or twice the loss or gain associated with the offense for trade secret theft and not more than the greater of $5 million or twice the loss or gain for economic espionage. Organizations are fined more severely, up to the greater of $5 million or twice the gain or loss for trade secret theft, and for economic espionage up to a fine 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. 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, but the EEA creates no explicit private cause of action. Conduct that violates the EEA's proscriptions may also violate other federal prohibitions, however. Some, like the Computer Fraud and Abuse Act, in addition to imposing criminal penalties, do authorize victims to sue for damages and other forms of relief under some circumstances.

# Stealing Trade Secrets

**Elements, Attempt, and Conspiracy:** The section's multiple elements limit its reach. The section condemns:

- Whoever
- with intent to convert
- a trade secret
- related to or included in a product that is produced for or placed 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 (a) steals ... , (b) without authorization copies ... downloads, uploads, alters, destroys, ... transmits ... sends, ... or conveys such information; [or] (c) 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.

*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" – "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; an act or series of acts of willful interference, without lawful justification, with any chattel in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the chattel." 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 merely inadvertent or otherwise innocent acquisition of a trade secret.

*Trade Secret*: A trade secret is any information of value, not publicly known, which "the owner thereof has taken reasonable measures to keep" secret. 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 with the statute's proscription.

*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.

*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 defined 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. And so, 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 manner necessary to satisfy the other elements of the offense.

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*: Defendants who attempt to steal a trade secret face the same penalties as those who succeed. Attempt consists of an intent to commit the offense and a substantial step towards the attainment of that goal. This suggests that the information which the defendant seeks to steal need not be a trade secret, as long as he believes it is.

*Conspiracy*: 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 the greater of $250,000 or twice the amount of any gain or loss associated with the offense. The court may fine a convicted organization up to the greater of $5 million or twice the amount of the gain or loss associated with the offense. Both individuals and organizations face a higher maximum fine if twice the gain or loss associated with the offense exceeds the statutory maximum (i.e., $250,000/$5 million). 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, but there is no explicit private cause of action.

# Economic Espionage

Economic espionage and theft of trade secrets share many of the same elements. There are four principal differences. The theft of trade secrets 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 $500,000 rather than $250,000. For organizations the maximum fine is $10 million 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.

Section 1831 condemns:

- Whoever
- intending or knowing the offense will benefit
- a foreign government, foreign instrumentality, or foreign agent
- knowingly
- (a) steals ... , (b) without authorization copies ... downloads, uploads, alters, destroys, ... transmits ... sends, ... or conveys such information; [or] (c) 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.

*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 further 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. It may also preclude prosecution when trial would have been possible in the

absence of an express provision. For example, in the absence of the limiting provision, the courts would allow prosecution of overseas offenses of foreign nationals that have an impact within the United States.

*Prosecutorial Discretion*: For five years after passage of the Economic Espionage Act, neither economic espionage nor trade secrets 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.

# Related Offenses

Conduct that violates the Economic Espionage Act may violate other federal criminal provisions as well. In the case of trade secrets offenses, potentially corresponding offenses include violations of the Computer Fraud and Abuse Act, the National Stolen Property Act, and the federal wire fraud statute. The Computer Fraud and Abuse Act outlaws accessing certain computers or computer systems without authorization or in excess of authorization, with the intent to defraud. The National Stolen Property Act outlaws the interstate transportation of tangible stolen property or the knowing receipt of such property. The federal wire fraud statute outlaws the use of wire communications in execution of a scheme to defraud.

In addition, in the case of economic espionage violations, a defendant may be charged under the general espionage laws, the espionage component of the computer fraud statute, or for failure to register as the agent of a foreign power. Foreign agents, other than diplomatic personnel, must register with the Attorney General; failure to do so is generally a felony. The Computer Fraud and Abuse Act outlaws computer intrusions launched for espionage purposes. The general espionage laws are only likely to be triggered if the trade secret information is also classified information or is national defense information.

# Amendments in the 112th Congress

Congress amended the EEA twice during the 112th Congress. The Theft of Trade Secrets Clarification Act of 2012 clarified the trade secrets jurisdictional element. The Foreign and Economic Espionage Act of 2012 increased the maximum fine levels for economic espionage. It also directed the United States Sentencing Commission to reexamine its treatment of economic espionage and the overseas transmission of stolen trade secrets.

## Stealing Trade Secrets

On November 27, 2012, Senator Leahy introduced, and the Senate passed by unanimous consent, the Theft of Trade Secrets Clarification Act (S. 3642). The proposal reworded the jurisdictional element of the trade secret provision to cover secrets relating to products or services used or intended for use in interstate or foreign commerce. Senator Leahy explained that:

> A recent decision of the Second Circuit in United States v. Aleynikov casts doubt on the reach of the statute. A jury in that case found the defendant guilty of stealing computer code from his employer. The court overturned the conviction, holding among other things that the trade secret did not meet the interstate commerce prong of the statute, even though the

> defendant had copied the stolen code from his office in New York to a server in Germany; downloaded the code to his home computer in New Jersey; then flew to his new job in Illinois with the stolen source code in his possession; and the code was used in interstate commerce.
>
> The court held that the Economic Espionage Act provision applies only to trade secrets that are part of a product that is produced to be placed in interstate commerce. Because the company's proprietary software was neither placed in interstate commerce nor produced to be placed in interstate commerce, the law did not apply – even though the stolen source code was part of the financial trading system that was used in interstate commerce every day.

The House passed the measure shortly thereafter under suspension of the rules, and the President signed it into law on December 28, 2012, P.L. 112-236.

## Economic Espionage

On August 1, 2012, the House passed the Foreign and Economic Espionage Penalty Enhancement Act of 2012 (H.R. 6029), under suspension of the rules. The Senate Judiciary Committee had previously reported favorably a similar proposal as the Economic Espionage Penalty Enhancement Act (S. 678). Unlike the Senate bill, the House legislation would have increased the penalties for violations of 18 U.S.C. 1831 (economic espionage). Under the House-passed proposal the maximum term of imprisonment would have increased from not more than 15 years to not more than 20 years. Section 1831 previously punished individual defendants with a fine of not more than the greater of $500,000 or twice the loss or gain associated with the offense and punished organizational defendants with a fine of not more than the greater of $10 million or twice the loss or gain. The House bill would have amended it to permit a fine for an offending individual of not more than the greater of $5 million or twice the loss or gain and to permit a fine for an offending organization of not more than the greater of $10 million, three times the value of the stolen trade secret, or twice the gain or loss associated with the offense.

Neither proposal would have changed the maximum terms of imprisonment (not more than 10 years) or the maximum fines for trade secret violations ($250,000 for individuals; $5 million for organizations). Both would have instructed the United States Sentencing Commission to reexamine the treatment of economic espionage and overseas transmission of stolen trade secrets under the Commission's sentencing guidelines.

The legislation is a reaction to reports of increased foreign predatory action and of "sensitive US economic information and technology ... targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries."

The Senate agreed to the House-passed proposal, but not before removing the provision that would have increased the length of the maximum prison term. The House agreed to the Senate amendment under suspension of the rules. The President signed the proposal on January 14, 2013, P.L. 112-269.

## Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968