Congressional Research Service
Informing the legislative debate since 1914

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

name redacted
Senior Specialist in American Public Law

August 19, 2016

Congressional Research Service
7-....
www.crs.gov
R42681

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, 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. Finally, by virtue of the Defend Trade Secrets Act (P.L. 114-153), Section 1831 and 1832 are predicate offenses for purposes of the federal racketeering and money laundering statutes.

P.L. 114-153 (S. 1890) 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 available in an abridged version, without footnotes or attribution, as CRS Report R42682, *Stealing Trade Secrets and Economic Espionage: An Abridged Overview of the Economic Espionage Act*.

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).[1] Under either proscription, its reach extends to theft from electronic storage.[2] Individual offenders face imprisonment for up to 15 years for economic espionage and up to 10 years for trade secret theft.[3] Individuals also may incur fines of up to $250,000 or twice the loss or gain associated with the offense for trade secret theft.[4] For economic espionage, they face fines of up $5 million or twice the loss or gain.[5] 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.[6] For economic espionage, the fines of 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.[7]

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.[8] 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.[9] The government may seek to enjoin violations,[10] and, by virtue of amendments in the Defend Trade Secrets Act of 2016,[11] victims may be entitled to sue for double damages, equitable relief, and attorneys' fees.[12]

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, likewise authorize victims to sue for damages and other forms of relief under some circumstances.[13]

[1] 18 U.S.C. §1831 (economic espionage) and 18 U.S.C. §1832 (theft of trade secrets).

[2] "Whoever ... without authorization ... downloads, uploads ... transmits ... or conveys such [trade secret] information," 18 U.S.C. §§1831(a)(2), 1832(a)(2)(same).

[3] 18 U.S.C. §§1832(a), 1831(a).

[4] 18 U.S.C. §§1832(a), 3571(c). Here and elsewhere, 18 U.S.C. §3571(d) provides as a general matter that the maximum for a criminal fine of any federal criminal offense is the greater of the standard amount set for the particular offense (*e.g.*, $250,000 for individuals convicted of a felony) or twice the gain or loss resulting from the offense.

[5] 18 U.S.C. §§1831(a), 3571(d).

[6] 18 U.S.C. §§1832(b), 3571(d).

[7] 18 U.S.C. §§1831(b), 3571(d).

[8] 18 U.S.C. §§1831(a)(4)(attempt), (5)(conspiracy), 1832(a)(4)(attempt), (5)(conspiracy); 2 (aiding and abetting).

[9] 18 U.S.C. §§1834 (forfeiture and restitution), 2323(c)(restitution), 2323(a)(civil forfeiture), 2323(b)(criminal forfeiture).

[10] 18 U.S.C. §1836.

[11] P.L. 114-153, §2, 130 Stat. 376 (2016).

[12] 18 U.S.C. §1836.

[13] *E.g.*, 18 U.S.C. §§1030(g)(computer fraud and abuse), 2520(interception of electronic communications), 2707 (unauthorized access to an electronic communications facility).

Stealing Trade Secrets

Elements

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

I.

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

or

II.

(1) Whoever
(2) attempts [to do so];

or

III.

(1) Whoever
(2) conspires with one or more other persons to [do so], and
(3) one or more of such persons do any act to effect the object of the conspiracy.[14]

[14] 18 U.S.C. §1832; *see also* United States v. Liu, 716 F.3d 159, 169-70 (5th Cir. 2013)("With respect to the substantive offense of theft of trade secrets, the Government must prove (1) that the defendant intended to convert proprietary information to the economic benefit of anyone other than the owner; (2) that the proprietary information was a trade secret; (3) that the defendant knowingly stole, copied, or received trade secret information; (4) that the defendant intended or knew the offense would injure the owner of the trade secret; and (5) that the trade secret was included in a product that is placed in [or is intended to be used in]interstate commerce"); U.S. Department of Justice, *Criminal Resource Manual* §1129 (May, 1999)(language in italics substituted to reflect P.L. 112-235's amendments) ("In order to establish a violation of 18 U.S.C. §1832, the government must prove: (1) the defendant stole, or without authorization of the owner, obtained, destroyed, or conveyed information; (2) the defendant knew this information was (continued...)

Substantive Offense

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."[15] 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."[16]

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 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."[17] 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

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."[18] 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."[19]

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

---

(...continued)

proprietary; (3) the information was in fact a trade secret; (4) the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner; (5) the defendant knew or intended that the owner of the trade secret would be injured; and (6) the trade secret was related to [*a product or service used in or intended for use in*] interstate or foreign commerce").

[15] 18 U.S.C. §1832.

[16] 1 U.S.C. §1 (emphasis added).

[17] BLACK'S LAW DICTIONARY 406 (10th ed. 2014).

[18] 18 U.S.C. 1839(3)("[T]the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if - (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, *another person who can obtain economic value from the disclosure or use of the information*"). The Defend Trade Secrets Act added the language in italics, P.L. 114-153, §2(b)(1)(A), 130 Stat. 380 (2016).

[19] 18 U.S.C. 1839(4).

access to the information and notifying employees of its confidential nature.[20] 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.[21]

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 more narrow 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."[22] The EEA definition initially referred to information known to or readily ascertainable by the "public."[23] 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."[24] The Defend Trade Secrets Act replaced the original definition with the UTSA language.[25]

[20] United States v. Chung, 659 F.3d 815, 825-29 (9th Cir. 2011)(citations omitted)("[R]easonable measures for maintaining secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on a 'need to know basis', and controlling plant access. Security measures, such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures"); United States v. Howley, 707 F.3d 575, 579 (6th Cir. 2013)("A reasonable jury could find that Goodyear took reasonable measures to keep the design of its tire-assembly machines secret. Goodyear surrounded its Topeka factory with a fence and required visitors to pass through a security checkpoint. Before [visitors] entered the factory, they had to obtain advance permission from Goodyear, sign confidentiality agreements and agree not to take photographs during their visit. And Goodyear required all of its suppliers … to keep Goodyear's proprietary information secret. ... The 'reasonable measures' requirement does not mean a company must keep its own employees and suppliers in the dark about machines they need to do their work").

[21] United States v. Krumrei, 258 F.3d 535, 539 (6th Cir. 2001); *see also* United States v. Genovese, 409 F. Supp. 2d 253, 257 (S.D.N.Y. 2005)(rejecting the contention that the "not ... generally known ... to the public" element of the definition of a trade secret was unconstitutionally vague as applied when the evidence showed that he clearly understood that the information he downloaded was not generally known).

[22] H.Rept. 104-788, at 12 (1996); *Chung*, 659 F.3d at 825.

[23] 18 U.S.C. §1839(3)(B)(2012 ed.).

[24] UNIF. TRADE SECRETS ACT §1(4), 14 U.L.A. 538 (2005). The Uniform Trade Secrets Act definition of trade secrets reads in its entirety: "'Trade Secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

[25] 18 U.S.C. §1839; H.Rept. 114-529, at 13-4 (2016)("The intent of §2(b)(1)(A) – striking 'the public' and inserting 'another person who can obtain economic value from the disclosure or use of the information'—is to bring the Federal definition of a trade secret into conformity with the definition used in the Trade Secrets Act ('UTSA'). Both the Court of Appeals for the Seventh Circuit in *United States v. Lange*, 312 F.3d 263, 267 (7th Cir. 2002), and the Court of Appeals for the Third Circuit, in *United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998), have identified this difference between the UTAS and the Federal definition of a trade secret as potentially meaningful. While other minor differences between the UTSA and Federal definition of a trade secret remain, the Committee does not intend for the definition of a trade secret to be meaningfully different from the scope of that definition as understood by courts in States that have adopted the UTSA.").

Related to a Product or Service 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.[26] 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.[27]

Economic Benefit of Another

Someone other than the trade secret's owner must be the intended beneficiary of the theft or destruction.[28] The thief may be, but need not be, the intended beneficiary.[29] 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.[30]

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.[31] However, it need not show actual injury.[32] 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."[33] 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.[34]

---

[26] 18 U.S.C. §1832(a)("Whoever, with intent to convert a trade secret that is related to *a product or service used in or intended for use in interstate or foreign commerce* ... "). United States v. Agrawal, 726 F.3d 235, 247 (2d Cir. 2013)(internal citations and some quotation marks omitted)("As the Supreme Court has recognized, the ordinary meaning of "related to" is broad: to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection.... The EEA's nexus provision creates no exception to an otherwise applicable general rule; rather, it signals Congress's intent to exercise its Commerce Clause authority to address the theft of trade secrets").

[27] United States v. Aleynikov, 676 F.3d 71, 80-2 (2d Cir. 2012)(construing 18 U.S.C. §1832(a) which at the time read: "Whoever, with intent to convert a trade secret that is related to *or included in a product that is produced for or placed* in interstate or foreign commerce ... ")(P.L. 112-236 struck the language in italics in favor of that quoted in italics in the previous footnote in order to overcome the implications of *Aleynikov*, 158 CONG. REC. S6978 (daily ed. Nov. 27, 2012)(introductory remarks of Sen. Leahy)).

[28] 18 U.S.C. §1832(a); United States v. Hsu, 155 F.3d 189, 195-96 (3d Cir. 1998); United States v. Jin, 833 F. Supp. 2d 977, 1016 (N.D. Ill. 2012), aff'd, 733 F.3d 718 (7th Cir. 2013).

[29] U.S. Department of Justice, Executive Office for United States Attorneys, *Prosecuting Intellectual Property Crimes (Justice Report)* 185 (4th ed. [2013])("The recipient of the intended benefit can be the defendant, a competitor of the victim, or some other person or entity").

[30] *Id.* ("One who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under [the section]").

[31] 18 U.S.C. §1832(a); *Jin*, 833 F.Supp.2d at 1018.

[32] United States v. Yihao Pu, 814 F.3d 818, 828 (7th Cir. 2016).

[33] H.Rept. 104-788, at 11-12 (1996), quoted in *Justice Report* at 185.

[34] *Cf.*, *Jin*, 733 F.3d at 721 ("The government doesn't have to prove that the owner of the secret actually lost money as a result of the theft. For remember that the independent economic value attributable to the information's remaining secret need only be 'potential,' as distinct from 'actual'").

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 Justice Department has used the section's legislative history to reinforce its understanding of this feature of the section:

> As outlined above, the first part of the *mens rea* requirement in an EEA case is that the defendant misappropriated the trade secret "knowingly." As noted in the legislative history, "A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and (2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by this statute." S. Rep No. 104-359, at 16 (1996).
>
> Based upon the legislative history, the government is not required to prove that the defendant knew and understood the statutory definition of a trade secret, as set forth in 18 U.S.C. § 1839(3), before acting. If the government had to prove this, the EEA would be unnecessarily narrowed in its application, which is contrary to the intent of Congress. Some violations would be nearly impossible to prosecute in a number of factual scenarios, and would amount to a willfulness *mens rea* requirement equivalent to that imposed for criminal copyright infringement. For example, as part of protecting and limiting a trade secret to those on a need to know basis, some companies do not divulge all of the reasonable measures used to protect the trade secret, even within the company. The individual stealing a trade secret may not know about these reasonable measures safeguarding the trade secret.
>
> The legislative history is clear that Congress intended to extend the reach of the new federal offenses involving trade secret misappropriation. In fact, the legislative history supports a "knew or should have known" *mens rea* requirement:
>
> > It is not necessary that the government prove that the defendant knew his or her actions were illegal, rather the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and that the defendant *knew or should have known* that fact.
>
> H.R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030-31 (emphasis added); 142 Cong. Rec. 27,117 (1996) (government must show the defendant was "aware or substantially certain" he was misappropriating a trade secret); *see also United States v. Genovese*, 409 F. Supp. 2d 253, 258 (S.D.N.Y. 2005) (discussing circumstances that would indicate that EEA defendant knew the information was proprietary).
>
> Congress did not require the government to show that the defendant specifically was aware of each element of the definition of a trade secret under § 1839(3) (e.g., that the defendant knew of specific reasonable measures employed by the trade secret owner to protect the trade secret). An opportunistic defendant, such as a company outsider, may not be fully aware of all of the company measures used to safeguard a trade secret, but does know the proprietary information has value which he intends to use to injure the owner of the trade secret. In other words, the defendant knowingly misappropriated property (or proprietary information) belonging to someone else without permission. In fact, in recognizing this point, the Sixth Circuit has held that the "defendant need not have been aware of the particular security measures taken by [the trade secret owner]. Regardless of his knowledge of those specific measures, defendant knew the information

> was proprietary." *Krumrei*, 258 F.3d at 539 (affirming denial of motion to dismiss indictment as void for vagueness); *see also United States v. Roberts*, No. 3:08-CR-175, 2009 WL 5449224, at *7 (E.D. Tenn. Nov. 17, 2009) (holding that "a defendant must know that the information he or she seeks to steal is proprietary, meaning belonging to someone else who has an exclusive right to it, but does not have to know that it meets the statutory definition of a trade secret"), *report and recommendation adopted by*, 2010 WL 56085 (E.D. Tenn. Jan. 5, 2010) (quoting H.R. Rep. No. 104-788, at 12 (1996)).[35]
>
> 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."[36]

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.[37]

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.[38] 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.[39] It makes the point with some trepidation, 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

---

[35] *Justice Report* at 177-79; *see also* United States v. Chung, 633 F. Supp. 2d 1134, 1143 (C.D. Cal. 2009), aff'd, 659 F.3d 815 (9th Cir. 2011)("It is not explicitly clear from the language of section 1831(a)(3)[which corresponds to section 1832(a)(3)] whether the word 'knowingly' modifies the 'trade secret' element of the offense. The Government argues that it does not, and therefore it does not have to prove that Mr. Chung knew that the information he possessed was a trade secret. Mr. Chung contends that the Government must prove that he had such knowledge. The Court agrees with Mr. Chung").

[36] United States v. Jin, 833 F. Supp. 2d 977, 1011-14 (N.D. Ill. 2012)), aff'd, 733 F.3d 718 (7th Cir. 2013); *Chung*, 633 F. Supp. 2d at 1145; *but see* United States v. Krumrei, 258 F.3d 535, 539 (6th Cir. 2001)(indicating that the government must show that the defendant knew the information was proprietary and thus by implication indicating that the government need not meet the higher standard of showing that he knew the information constituted a trade secret).

[37] 18 U.S.C. §1832(a)(1)(" ... [K]nowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information").

[38] 18 U.S.C. §1832(a)(2)("[K]nowingly ... (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information").

[39] *Justice Report* at 175-76 ("The statute also prohibits not only actions taken against a trade secret's physical form, such as 'steal[ing], ...tak[ing], [and] carr[ying] away', 18 U.S.C. §§1831(a)(1), 1832(a)(1), but also actions that can be taken against a trade secret in a memorized, intangible form, such as 'sketch[ing], draw[ing], ... download[ing], upload[ing], ..., transmit[ting], ... communicat[ing], [and] convey[ing],' 18 U.S.C. §§1831(a)(2), 1832(a)(2). See James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997). In this respect, as in others, the EEA echoes civil law and some pre-EEA case law. *See, e.g.* , 4 Roger M. Milgrim, MILGRIM ON TRADE SECRETS §15.01[e]; Stampede Tool Warehouse v. May, 651 N.E.2d 209, 217 (Ill. App. Ct. 1995) ('A trade secret can be misappropriated by physical copying or by memorization.') (citations omitted). Trade secret cases to the contrary that do not involve the EEA are thus not persuasive authority on this point"). *See also Thirty-First Annual Survey of White Collar Crime: Intellectual Property Crimes*, 53 AM. CRIM. L. REV. 1459 (2016).

> 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."[40]

The third subsection outlaws the knowing receipt of stolen trade secret information.[41] 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.[42]

Attempt

Defendants who attempt to steal a trade secret face the same penalties as those who succeed.[43] Attempt consists of intent to commit the offense and a substantial step toward the attainment of that goal.[44] 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.[45]

Conspiracy

Defendants who conspire to steal a trade secret also face the same penalties as those who commit the substantive offense.[46] "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."[47] 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.[48]

---

[40] *Justice Report* at 155.

[41] 18 U.S.C. §1832(a)(3)("... [K]nowingly ... (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization").

[42] 18 U.S.C. §1832(a)(3); United States v. Jin, 833 F. Supp. 2d 977, 1015 (N.D. Ill. 2012), aff'd, 733 F.3d 718 (7th Cir. 2013).

[43] 18 U.S.C. §1832(a).

[44] United States v. Hsu, 155 F.3d 189, 202-203 (3d Cir. 1998); United States v. Lange, 312 F.3d 263, 268 (7th Cir. 2002); United States v. Yang, 281 F.3d 534, 543 (6th Cir. 2002).

[45] *Hsu*, 155 F.3d at 203 ("It naturally follows that the government need not prove that an actual trade secret was used during the EEA investigation, because the defendant's culpability for a charge of attempt depends only on the 'circumstances as he believes them to be,' not as they really are"); *Yang*, 281 F.3d at 543-44 ("The Yangs believed that the information Lee was providing was trade secrets belonging to Avery. They attempted to steal that information. The fact that they actually did not receive a trade secret is irrelevant"); *cf.*, United States v. Nosal, ___ F.3d ___, ___ *16 (9th Cir. July 5, 2016); *but see Lange*, 312 F.3d at 269 ("But it is far less clear that [the] sale of information already known to the public could be deemed a substantial step toward the offense, just because the defendant is deluded and does not understand what a trade secret is.... We need not pursue the subject beyond noting the plausibility of the claim and its sensitivity to the facts – what kind of data did the employee think he stole, and so on. For it is not necessary to announce a definitive rule about how dangerous the completed acts must be in trade secret cases: the judge was entitled to (and did) find that Lange had real trade secrets in his possession").

[46] 18 U.S.C. §1832(a).

[47] *United States v. Martin*, 228 F.3d 1, 10-11 (1st Cir. 2000); cf., *United States v. Chung*, 659 F.3d 815, 828-29 (9th Cir. 2011).

[48] *Hsu*, 155 F.3d at 203-204; *Yang*, 281 F.3d at 544.

Consequences

Individual offenders face imprisonment for up to 10 years and fines of up to $250,000.[49] The court may fine an organization up to $5 million upon conviction.[50] 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).[51] A sentencing court must also order the defendant to pay restitution to the victims of the offense.[52] Property derived from, or used to facilitate, commission of the offense may be subject to confiscation under either civil or criminal forfeiture procedures.[53] The Attorney General may sue for injunctive relief, and owners may sue for damages, equitable relief, and attorneys' fees.[54] Finally, the offense is a RICO predicate offense[55] and consequently a money laundering predicate offense.[56]

Economic Espionage

The EEA's economic espionage and theft of trade secret offenses share many of the same elements.[57] There are four principal differences. The theft of a trade secret must involve the intent to benefit someone other than the owner.[58] It must involve an intent to injure the owner.[59] 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."[60] 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.[61] It does not require an intent to injure the owner.[62] And, it applies to any trade secret, notwithstanding the absence of any connection to interstate or foreign commerce.[63] Finally, economic espionage is punished more severely. The maximum term of imprisonment is 15 years

[49] 18 U.S.C. §§1832(a), 3571.

[50] 18 U.S.C. §1832(b).

[51] 18 U.S.C. 3571(d).

[52] 18 U.S.C. §§1834, 2323(c), 3663A(a), (c). *See generally* CRS Report RL34138, *Restitution in Federal Criminal Cases*.

[53] 18 U.S.C. §§1834, 2332(a), (b). *See generally* CRS Report 97-139, *Crime and Forfeiture*.

[54] 18 U.S.C. §1836.

[55] RICO makes it a federal crime, among other things, to conduct the affairs of commercial enterprise through the patterned commission of a series of federal or state crimes (predicate offenses), 18 U.S.C. §§1961-1963. *See generally* CRS Report 96-950, *RICO: A Brief Sketch*.

[56] 18 U.S.C. §§1956(c)(7)(A), 1957(f)(3). Section 1957 makes it a federal crime to engage in a monetary transaction using property generated by a predicate offense worth more than $10,000. Section 1956 makes it a federal crime to launder the proceeds of a predicate offense or to use them to promote further offenses. *See generally* CRS Report RL33315, *Money Laundering: An Overview of 18 U.S.C. 1956 and Related Federal Criminal Law*.

[57] 18 U.S.C. §§1831, 1832.

[58] 18 U.S.C. §1832(a).

[59] *Id.*

[60] *Id.*

[61] 18 U.S.C. §1831(a)("Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent ... "); United States v. Jin, 833 F. Supp. 2d 977, 1019 (N.D. Ill. 2012), aff'd, 733 F.3d 718 (7th Cir. 2013).

[62] *Id.*

[63] *Id.*; United States v. Aleynikov, 676 F.3d 71, 79 (2d Cir. 2012)("Thus there is a limitation – [a nexus to] interstate or foreign commerce – in the statute Aleynikov is charged with violating, a limitation that does not appear in the otherwise parallel foreign espionage statute").

rather than 10 years, and the maximum fine for individuals is $5 million rather than $250,000.[64] For organizations, the maximum fine is the greater of $10 million or three times the value of the trade secret rather than $5 million.[65] 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.[66] And the crime is likewise a RICO and, consequently, a money laundering predicate offense.[67]

Section 1831 condemns:

I.

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

or

II.

(1) Whoever
(2) attempts [to do so];

or

III.

(1) Whoever
(2) conspires with one or more other persons to [do so], and
(3) one or more of such persons do any act to effect the object of the conspiracy.[68]

[64] 18 U.S.C. §§1831(a), 1832(a).

[65] 18 U.S.C. §§1831(b), 1832(b).

[66] 18 U.S.C. §3571(d).

[67] 18 U.S.C. §§1961(1), 1956(c)(7)(A), 1957(f)(3).

[68] 18 U.S.C. §1831; *see also* United States v. Chung, 633 F. Supp. 2d 1134, 1146 (C.D. Cal. 2009), aff'd, 659 F.3d 815 (9th Cir. 2011)("Accordingly, under section 1831(a)(3), the Government must prove five elements: (1) Mr. Chung intended to benefit a foreign government; (2) Mr. Chung knowingly possessed trade secret information; (3) Mr. Chung knew the information was obtained without authorization; (4) the information Mr. Chung possessed was, in fact, a trade secret; and (5) Mr. Chung knew the information was a trade secret"); U.S. Department of Justice, Criminal Resource Manual §1124 ("In order to establish a violation of 18 U.S.C. §1831, the government must prove: (1) the defendant stole or, without authorization of the owner, obtained, destroyed, or conveyed information; (2) the defendant knew this information was proprietary; (3) the information was in fact a trade secret; and (4) the defendant knew the offense would benefit or was intended to benefit a foreign government, foreign instrumentality, or foreign agent").

Foreign Beneficiary

A casual reader might conclude that any foreign entity would satisfy Section 1831's foreign beneficiary element.[69] 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.[70] The description of a foreign agent leaves no doubt that the individual or entity must be the agent of a foreign government.[71]

The theft of a trade secret demands an intent to confer an economic benefit.[72] Economic espionage is not so confined. Here, "benefit means not only economic benefit but also reputational, strategic, or tactical benefit."[73] 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.[74] As in the case of trade secret theft, however, the benefit need not be realized; it is enough that defendant intended to confer it.[75]

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.[76] The government may not appeal an order to reveal information it has already

[69] 18 U.S.C. §1831(a)(" ... [I]ntending or knowing the offense will benefit (3) (a) a foreign government, (b) a foreign instrumentality, or (c) a foreign agent ... ").

[70] 18 U.S.C. §1839(1)("As used in this chapter – (1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government").

[71] 18 U.S.C. §1839(1)("As used in this chapter ... (2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government").

[72] 18 U.S.C. §1832(a)("Whoever, with the intent to convert a trade secret ... to the economic benefit of anyone other than the owner ... ").

[73] H.Rept. 104-788, at 11 (1996).

[74] 18 U.S.C. §§1832(a)("Whoever, with the intent to convert a trade secret ... to the economic benefit of anyone other than the owner ... "); 1831(a)("Whoever, intending or knowing that the offense will benefit ... ").

[75] *Id.*

[76] 18 U.S.C. §1835; United States v. Hsu, 155 F.3d 189, 193-94 (3d Cir. 1998).

disclosed to the defendant.[77] Nevertheless, in such instances, appellate review of a district court's disclosure order may be available through a writ of mandamus.[78]

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.'"[79] 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.[80] 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.[81]

The legislative history indicates that these are the only circumstances under which violations abroad may be prosecuted.[82] This may mean that foreign conspirators may not be charged unless some overt act in furtherance of the scheme occurs in the United States.[83] 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 likely conclude that Congress

[77] United States v. Ye, 436 F.3d 1117, 1120-121 (9th Cir. 2006)("The plain language of the EEA indicates that the government can file an interlocutory appeal pursuant to §1835 only where a district court's order actually directs or authorizes the disclosure of a trade secret.... Here, the district court's order did not provide for the disclosure of any trade secret materials. In its opening brief in this court, the government acknowledges that it had already turned over all relevant trade secret materials and documents.... Because the purpose of the district court's order was only to clarify exactly which materials the government contends constitute the protected trade secrets, and all relevant materials had already been turned over, the district court's order does not direct or authorize the 'disclosure' of trade secrets as required by the plain language of §1835").

[78] *Id.* at 1121-124. Mandamus relief is a discretionary remedy ordinarily only available when the petitioner can show: the absence of any other form of relief, a clear right to issuance of the writ, and that recourse to this extraordinary form of relief is appropriate under the circumstances, Cheney v. United States District Court, 542 U.S. 367, 380-81 (2004). The lower federal appellate courts sometimes describe these requirements in greater detail, see e.g., *Lewis v. Ayers*, 681 F.3d 992, 998 (9th Cir. 2012)("In *Bauman*, we established five guidelines to determine whether mandamus is appropriate in a given case:(1) whether the petitioner has no other means, such as a direct appeal to obtain the desired relief; (2) whether the petitioner will be damaged or prejudiced in any way not correctable on appeal; (3) whether the district court's order is clearly erroneous as a matter of law; (4) whether the district court's order is an oft repeated error or manifests a persistent disregard of the federal rules; and (5) whether the district court's order raises new and important problems or issues of first impression"); In re Jones, 680 F.3d 640, 642 (6th Cir. 2012)(essentially the same).

[79] Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010), quoting EEOC v. Arabian American Oil Co., 449 U.S. 244, 248 (1991) and Foley Bros., Inc. v. Filardo, 336 U.S. 281 (1949). *See generally* CRS Report 94-166, *Extraterritorial Application of American Criminal Law*.

[80] H.Rept. 104-788, at 14 (1996).

[81] 18 U.S.C. 1837 ("This chapter also applies to conduct occurring outside the United States if - (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States").

[82] H.Rept. 104-788, at 14 (emphasis added)("To ensure that there is some nexus between the ascertaining of such jurisdiction and the offense, however, extraterritorial jurisdiction exists *only* if [an overt act occurs within the United States or the offender is a U.S. national]").

[83] 18 U.S.C. §1837 (emphasis added)("This chapter also applies to conduct occurring outside the United States if - (1) the *offender* is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States").

intended to allow prosecution of overseas offenses of foreign nationals that have an impact within the United States.[84]

Prosecutorial Discretion

For five years after passage of the Economic Espionage Act, 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.[85]

Related Offenses

Conduct that violates the Economic Espionage Act may violate other federal criminal provisions as well. In the case of trade secret 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.[86] The National Stolen Property Act outlaws the interstate transportation of tangible stolen property

[84] *Ford v. United States*, 273 U.S. 593, 623 (1927)("A man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done"); *United States v. Yousef*, 327 F.3d 56, 96-7 (2d Cir. 2003)("Moreover, assertion of jurisdiction is appropriate under the 'objective territorial principle,' because the purpose of the attack was to influence United States foreign policy and the defendant intended their actions to have an effect – in this case a devastating effect—on and within the United States"); *United States v. Felix-Gutierrez*, 940 F.2d 1200, 1205 (9th Cir. 1991)(Felix's actions created a significant detrimental effect in the United States ..."). See also *The Extraterritorial Application of the Economic Espionage Act of 1996*, 23 HASTINGS INT'L & COMP. L. REV. 527, 553-54 (2000)("If a foreign company possesses no operations in the U.S. and engages in trade secret theft against a U.S. entity entirely outside the U.S., then EEA cannot apply. In that respect, the extraterritorial jurisdiction under the EEA may fall short of the jurisdictional reach applied under a 'pure' effects test in antitrust law – where the Sherman Act can reach conduct entirely extraterritorial in nature").

[85] U.S. Department of Justice, *Criminal Resource Manual* §1122 ("Prior to passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice would require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General to the Criminal Division. (See October 1, 1996 letter from Attorney General Janet Reno to Chairman Orrin Hatch, *Criminal Resource Manual* at 1123). This requirement expired on October 11, 2001. Subsequently, the Attorney General renewed the prior requirement for initiating prosecutions under 18 U.S.C. §1831.... The requirement was not extended for cases under 18 U.S.C. §1832 ... ").

[86] 18 U.S.C. §1030(a)(4), (e)(2)("(a) Whoever ... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period ... shall be punished as provided in subsection (c) of this section.... (e) As used in this section ... (2) the term 'protected computer' means a computer - (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"); *e.g.*, United States v. Nosal, ___ F.3d ___, ___*2 (9th Cir. July 5, 2016)(defendant convicted computer fraud and theft of trade secrets); United States v. Koo, 770 F.Supp.2d 1115, 1118 (D. Or. 2011)(defendant indicted for computer fraud and abuse and for trade secrets violations); United States v. Pu, 15 F. Supp. 3d 846, 849 (N.D. Ill. 2014)(defendant indicted for trade secret, computer fraud and wire fraud violations); *see generally* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*.

or the knowing receipt of such property.[87] The federal wire fraud statute outlaws the use of wire communications in execution of a scheme to defraud.[88]

In addition, in the case of economic espionage violations, a defendant may be subject to prosecution under the general espionage statutes, 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.[89] The Computer Fraud and Abuse Act outlaws computer intrusions launched for espionage purposes.[90] The general espionage laws are only likely to be triggered if the trade secret information is also classified information or national defense information.[91]

[87] 18 U.S.C. §2314 ("Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted, or taken by fraud.... shall be fined under this title or imprisoned not more than ten years or both ... "); 18 U.S.C. §2315("Whoever receives, possesses, conceals, stores, barters, sells, or dispose of any goods, ware, or merchandise, securities, or money of the value of $5,000 or more ... which have crossed a State of United States boundary after being stolen ... knowing the same to have been stolen ... shall be fined under this title or imprisoned not more than ten years, or both"); *see also* United States v. Aleynikov, 676 F.3d 71, 76-9 (2d Cir. 2012)(stolen, intangible computer source code is neither a good, ware, nor merchandise for purposes of the National Stolen Property Act); United States v. Agrawal, 726 F.3d 235, 262 (2d Cir. 2013)(affirming trade secrets and stolen property convictions under 18 U.S.C. §1832 and 18 U.S.C. §2314).

[88] 18 U.S.C. §1343 ("Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire ... any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both ... "); *e.g.*, United States v. Hsu, 155 F.3d 189, 193 (3d Cir. 1998)(defendant indicted for wire fraud and trade secrets violations); *Koo*, 770 F.Supp.2d at 1118 (same*); see generally* CRS Report R41930, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law*.

[89] 18 U.S.C. §951(a)("Whoever, other than a diplomatic or consular officer or attaché, acts in the United States as an agent of a foreign government without prior notification to the Attorney General if required in subsection (b), shall be fined under this title or imprisoned not more than ten years, or both"); *e.g.*, United States v. Chung, 659 F.3d 815, 819 (9th Cir. 2011)(defendant indicted for economic espionage and unregistered foreign agent violations).

[90] 18 U.S.C. §1030(a)("Whoever- (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it ... shall be punished as provided in subsection (c) of this section.... (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. (c) The punishment for an offense under subsection (a) or (b) of this section is - (1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph. ... ").

[91] 18 U.S.C. §798, outlaws the unauthorized disclosure of classified information relating to communications intelligence; 18 U.S.C. §1924 outlaws the unauthorized retention of classified information; and 18 U.S.C. §§793, 794 outlaw the unauthorized gathering or transmitting of national defense information; *see generally* CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*.

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.[92] The Defend Trade Secrets Act created a private cause of action.[93]

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."[94] Not just anyone who suffers damage as the result of trade secret misappropriation; "owners" may sue. EEA, however, defines the term "owners" to include licensees.[95] The trade secrets protected by civil suit are the same as those protected by the criminal proscriptions.[96] The definition of the action that gives rise to liability – "misappropriation" – is taken from the Uniform Trade Secrets Act.[97] The term encompasses acquiring, disclosing, or using a trade secret taken from its owner by scurrilous ("improper") means.[98]

Pre-Trial Seizure

Perhaps 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

[92] P.L. 104-294, §101, 110 Stat. 3490 (1996), codified, as amended, 18 U.S.C. §1836(a).

[93] P.L. 114-153, §2, 130 Stat. 376 (2016), codified at 18 U.S.C. §1836(b).

[94] *Id.*

[95] 18 U.S.C. §1839(4)("[T]he term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed….").

[96] 18 U.S.C. §1839("As used in this chapter …(3) the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information").

[97] H.Rept. 114-529, at 14 (2016)("'[M]isappropriation' is defined identically in all relevant respects to the definition of misappropriation in §1(2) of the UTSA").

[98] 18 U.S.C. §1839("(5) [T]he term 'misappropriation' means - (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who – (i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was - (I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that - (I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake; [and]

"(6) [T]he term 'improper means'- (A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition….").

seizing the purported trade secret.[99] 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.[100] Yet, the procedure is confined to instances where a TRO is insufficient.[101] "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."[102]

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.[103] Anyone injured by a "wrongful or excessive" seizure may sue for the relief described in the Trademark Act;[104] 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," and, in the discretion of the court, prejudgment interest.[105]

Damages and Equitable Relief

Relying heavily on the UTSA, EEA empowers district courts to award an aggrieved owner equitable relief;[106] damages;[107] and in case of willful and malicious misappropriation, double

[99] 18 U.S.C. §1836(b)(2)(A)(i)("Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret….").

[100] 18 U.S.C. 1836(b)(2)(A)(ii)("The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that- (I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order; (II) an immediate and irreparable injury will occur if such seizure is not ordered; (III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure; (IV) the applicant is likely to succeed in showing that - (aa) the information is a trade secret; and (bb) the person against whom seizure would be ordered - (AA) misappropriated the trade secret of the applicant by improper means; or (BB) conspired to use improper means to misappropriate the trade secret of the applicant; (V) the person against whom seizure would be ordered has actual possession of - (aa) the trade secret; and (bb) any property to be seized; (VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized; (VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and (VIII) the applicant has not publicized the requested seizure.").

[101] 18 U.S.C. 1836(b)(2)(A)(ii)("The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that - (I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure [relating to preliminary injunctions and temporary restraining orders] or another form of equitable relief would be inadequate to achieve the purpose of this paragraph….").

[102] S.Rept. 114-220, at 6 (2016).

[103] 18 U.S.C. §1836(b)(2)(B)(v), (b)(2)(F)(ii).

[104] 18 U.S.C. §1836(b)(2)(G).

[105] 15 U.S.C. §1116(d)(11).

[106] 18 U.S.C. §1836(c), (b)(3)("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may - (A) grant an injunction - (i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not - (I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business; (ii) if determined (continued...)

damages and attorneys' fees.[108] The court may also award attorneys' fees to a party who prevails against a bad faith claim of misappropriation.[109]

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.[110]

Section 1837 states that the chapter 90 applies to conduct occurring outside the United States if "the offender" is a U.S. national or an act in furtherance of the offense is committed within the United States. Section 1836 is found in chapter 90. It would therefore appear that Section 1836 applies to conduct occurring outside the United States if the offender is a U.S. national or an act in furtherance of the offense is committed within the United States. In the absence of a Section 1837-like statement of congressional intent, the Supreme Court has shown a great reluctance to recognize private causes of action based on conduct abroad.[111] Whether the concerns evidenced there influence future extraterritorial application of Section 1836's civil remedies remains to be seen.

Author Contact Information

(name redacted)
Senior Specialist in American Public Law
[redacted]@crs.loc.gov, ...

(...continued)

appropriate by the court, requiring affirmative actions to be taken to protect the trade secret; and (iii) in exceptional circumstances that render an injunction inequitable, that conditions future use of the trade secret upon payment of a reasonable royalty for no longer than the period of time for which such use could have been prohibited").

[107] 18 U.S.C. §1836(b)(3)(B)("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may – (B) award - (i)(I) damages for actual loss caused by the misappropriation of the trade secret; and (II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or (ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret"). *Note*, S.Rept. 114-220, at 9 and in brackets n.17 of the report ("It is not the Committee's intent to encourage the use of reasonable royalties to resolve trade secret misappropriation. Rather, the Committee prefers other remedies that, first, halt the misappropriator's use and dissemination of the misappropriated trade secret and, second, make available appropriate damages. [The Committee notes that courts interpreting the UTSA's analogous provision have held that the award of reasonable royalties is a remedy of last resort].").

[108] 18 U.S.C. §1836(b)(3)(C)("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may …(C) if the trade secret is willfully and maliciously misappropriated, award exemplary damages in an amount not more than 2 times the amount of the damages awarded under subparagraph (B); and (D) if … the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.").

[109] 18 U.S.C. §1836(b)(3)(D).

[110] 18 U.S.C. §1836(d).

[111] *E.g.*, RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2016, 2111 (2016) (civil racketeering statute does not apply to injuries inflicted overseas); Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1669 (2013) (the Alien Tort Statute does not extraterritorially); Morrison v. National Australia Bank Ltd., 561 U.S. 247, 273 (2010) (Section 10(b) of the Securities Exchange Act of 1934, which creates a civil cause of action of misconduct relating to securities trading, does not apply to misconduct occurring abroad and relating to securities not listed on an American exchange).