Skadden

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

January 3, 2013

Recent Amendment to the Economic Espionage Act Extends Protection Against Misappropriation

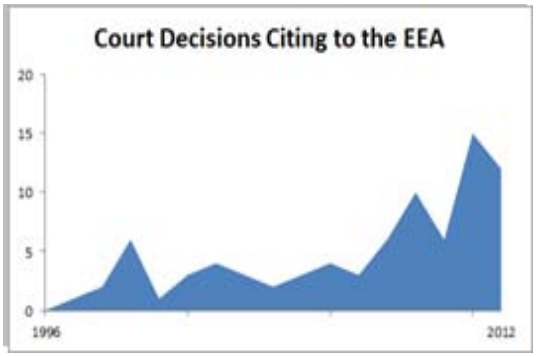
On December 28, 2012, President Obama enacted the Theft of Trade Secrets Clarification Act of 2012 (the Act). The Act clarifies the scope of Section 1832 of the Economic Espionage Act of 1996 and attempts to reverse the Second Circuit's recent decision in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). Significantly, the Act clarifies that the EEA protects wholly internal proprietary information if the information relates to products or services that are used in interstate or foreign commerce.

Economic Espionage Act of 1996

The Economic Espionage Act of 1996 (EEA), 18 U.S.C. §§ 1831-39, protects proprietary economic information by making certain types of trade secret misappropriation federal crimes.

Congress enacted the EEA to provide "a systematic approach to the problem of economic espionage." The EEA was designed to reflect the increasing importance of "intangible assets" like trade secrets in the "high-technology, information age," as well as the growing threat posed by the theft of such proprietary information and the inadequacy of existing federal laws to protect trade secrets. H.R. Rep. No. 104-788, at 4-7 (1996); *see also* S. Rep. No. 104-359, at 6-11 (1996).

The EEA created two offenses: "economic espionage" under Section 1831 and "theft of trade secrets" under Section 1832.



For either offense to apply, the defendant must have knowingly: (a) obtained a trade secret without authorization, such as by theft or fraud; (b) copied, altered or transmitted a trade secret without authorization; or (c) received a trade secret, knowing that the information was stolen or obtained without authorization. *See* 18 U.S.C. §§ 1831-32.

A conviction under Section 1831 for economic espionage further requires that the individual intend or know that the offense would "benefit any foreign government, foreign instrumentality, or foreign agent[.]" 18 U.S.C. § 1831(a). Individuals convicted under Section 1831 may be fined up to $500,000 and imprisoned up to 15 years. 18 U.S.C. § 1831(a). Organizations can be fined up to $10 million. 18 U.S.C. 1831(b).[1]

1 Pending legislation may soon enhance penalties for violations of Section 1831 of the EEA. The Foreign and Economic Espionage Penalty Enhancement Act of 2012, H.R. 6029, 112th Cong. (2012), would increase the minimum fine for an individual to $5 million and for organizations to the greater of $10 million or three times the value of the stolen trade secrets to the organization. On January 1, 2013, the House approved the Senate's amendments to H.R. 6029, which currently awaits the President's signature to be enacted.

By contrast, a conviction under Section 1832 for theft of trade secrets does not require that the defendant intended the action to benefit a foreign entity. Instead, Section 1832 requires evidence that the defendant intended to benefit "anyone other than the owner thereof," while also "intending and knowing that the offense will … injure the owner of that trade secret." 18 U.S.C. § 1832(a).

Most importantly, Section 1832 also requires that the trade secret "relate … to or [be] included in *a product* that is produced for or placed in interstate or foreign commerce. …" *See* 18 U.S.C. § 1832 (a) (emphasis added).

Individuals convicted under Section 1832 can be sentenced up to 10 years in prison and/or fined. 18 U.S.C. § 1832(a). Organizations can be fined up to $5 million. 18 U.S.C. § 1832 (b).

United States v. Aleynikov

In April 2012, the Second Circuit reversed a conviction under the EEA after determining that the misappropriated trade secrets were not sufficiently related to a product produced for or placed in interstate or foreign commerce, as required under Section 1832(a).

The defendant, Sergey Aleynikov, was a former computer programmer and vice president in Equities at Goldman Sachs. While at Goldman Sachs, Aleynikov was responsible for developing computer programs used in the bank's high-frequency trading (HFT) system . The HFT system used statistical algorithms to analyze past trades and market developments.[2] Goldman Sachs treated the system as proprietary information and implemented various security measures to keep it secret. Among other measures, the bank required employees to sign confidentiality agreements and limited employee access to the source code.

On his last day of employment at Goldman Sachs, Aleynikov copied, encrypted and transferred to a server in Germany the source code for the HFT system, including the algorithms that determined the value of stock options. *See United States v. Aleynikov*, 737 F. Supp. 2d 173, 175 (S.D.N.Y. 2010). Aleynikov later downloaded the source code from the German server to his home computer in the United States, flew to Chicago, Illinois, and brought the source code with him to a meeting with a Goldman Sachs competitor.

In February 2010, Aleynikov was indicted for, among other offenses, theft of trade secrets under 18 U.S.C. § 1832 for misappropriating Goldman Sach's source code. *United States v. Aleynikov*, 737 F. Supp. 2d 173, 174 (S.D.N.Y. 2010). Aleynikov moved to dismiss the theft of trade secrets count, arguing that Section 1832(a) only applies to trade secrets "relating to tangible products actually sold, licensed or otherwise distributed." *See id.* at 177. The source code, he argued, was never intended to be placed in interstate or foreign commerce. *See id.* at 180.

The district court disagreed, finding that the HFT system was a "product" that was "produced for" interstate commerce. "Indeed, the sole purpose for which Goldman purchased, developed, and modified the computer programs … was to engage in interstate and foreign commerce." *See United States v. Aleynikov*, 737 F. Supp. 2d 173, 179 (S.D.N.Y. 2010). Furthermore, the court found that the legislative history indicated that Congress "intended for the EEA to provide 'comprehensive' and 'systematic' protection for trade secrets belonging to companies in the United States, not just manufacturers of tangible consumer products." *See United States v. Aleynikov*, 737 F. Supp. 2d 173, 181 (S.D.N.Y. 2010). At trial, the jury convicted Aleynikov of two violations of federal law, including theft of

---

2 The proprietary computer programs included three kinds: (1) programs that process real-time market data and execute trades; (2) programs that use algorithms to determine which trades to make; and (3) infrastructure programs that facilitate the flow of information through the trading system. *See United States v. Aleynikov*, 676 F.3d 71, 82 (2d Cir. 2012).

trade secrets. *United States v. Aleynikov*, No. 10 Cr. 096, 2011 U.S. Dist. LEXIS 40424, 2011 WL 1334850, at *1 (S.D.N.Y. Mar. 28, 2011). Aleynikov was sentenced to 97 months' imprisonment. *Id.* at *3.

Aleynikov appealed his conviction and reiterated the argument that the source code was not related to a product "produced for or placed in interstate or foreign commerce" within the meaning of the EEA. *See United States v. Aleynikov*, 676 F.3d 71, 75 (2d Cir. 2012).

The Second Circuit reversed the district court and agreed with Aleynikov that the EEA did not apply to the source code. *Id.* at 76. The Court found that "Goldman's HFT system was neither 'produced for' nor 'placed in' interstate or foreign commerce" because "Goldman had no intention of selling its HFT system or licensing it to anyone." *See id.* at 82. The Court recognized that the decision appeared to be at odds with the Congressional intent behind the EEA and expressed its hope that Congress would amend the Act appropriately. *See, e.g.*, *id.* at 83 (Calabresi, J., concurring).

Theft of Trade Secrets Act of 2012

In response to the Second Circuit's decision, the Senate introduced the Theft of Trade Secrets Act of 2012, S. 3642, 112th Cong. (2012), to clarify the scope of the EEA. On November 27, 2012, the Senate unanimously passed the bill and, on December 18, 2012, the House passed an identical version by a vote of 388 to 4. President Obama signed the bill on December 28, 2012, enacting the amendment into law.

18 U.S.C. § 1832 (as amended)

(a) Whoever, with intent to convert a trade secret, that is related to ~~or included in a product that is produced for or placed in~~ a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly — . . . .

As amended, Section 1832 (a) will require that the trade secret relate to a product *or service* that is *used* or *intended for use* in interstate or foreign commerce. The offense will no longer be limited to theft of trade secrets related to a *product* that is *produced for or placed in* interstate or foreign commerce.

The intended consequence of the amendment will be to reject the Second Circuit's interpretation of the scope of the EEA. *See, e.g.*, 158 Cong. Rec. H6849 (daily ed. Dec. 18, 2012) (statement of Rep. Smith) (noting the "dangerous loophole" created by the *Aleynikov* decision and calling on Congress to "take action in response to the Second Circuit's call and to ensure we have appropriately adapted the scope of the EEA to the digital age").

The broader scope, combined with the recent publicity of the *Aleynikov* case, will likely spur an increase in criminal indictments under the EEA as companies increasingly recognize the Act as a powerful weapon in defense of trade secrets.

Practical Guidance

For companies seeking to protect trade secrets, the amended EEA may be an attractive alternative to litigating claims in state court. Like state trade secret law, the EEA can be invoked against organizations as well as individuals, but unlike state law, the EEA creates federal jurisdiction to move the case into federal, rather than state, court. In addition, federal prosecutors may have more success at protecting the victim's confidential information than a potentially less-sympathetic plaintiff in a civil action. *See, e.g.*, 18 U.S.C. § 1835 (Orders to Preserve Confidentiality). Finally, the EEA can

also provide a stronger deterrent than corresponding civil remedies. Former employees, for example, may be less willing to risk 10 years in federal prison than a few years' injunction against working with a competitor.

On the other hand, the broad scope of the EEA applies to more than just intentional theft and, broadly applied, may become a significant hazard for companies that legitimately receive the confidential information of another. In civil litigation, for example, many defendants are surprised to learn that activities they believed were lawful methods for gathering business intelligence or research and development leads may in fact constitute acts of trade secret misappropriation. Part of the confusion is attributable to the fact that a trade secret can be virtually any type of information, including combinations of public information. Furthermore, misappropriation can occur simply by exceeding authorization. Even for sophisticated parties, authorization can sometimes be difficult to determine.

Companies should therefore invest in understanding the basics of trade secret law and how to properly handle the confidential or proprietary information of another. Failure to do so may not only subject the company to civil liability, but federal criminal liability as well.

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Palo Alto Office
525 University Ave. | Suite 1100 | Palo Alto, CA 94301

James J. Elacqua | Partner
650.470.4510 | james.elacqua@skadden.com

David W. Hansen | Partner
650.470.4560 | david.hansen@skadden.com

Andrew N. Thomases | Partner
650.470.4580 | andrew.thomases@skadden.com

New York Office
4 Times Square | New York, NY 10036

Daniel A. DeVito | Partner
212.735.3210 | daniel.devito@skadden.com

Edward V. Filardi | Partner
212.735.3060 | edward.filardi@skadden.com

Douglas R. Nemec | Partner
212.735.2419 | douglas.nemec@skadden.com

P. Anthony Sammi | Partner
212.735.2307 | anthony.sammi@skadden.com

Stacey L. Cohen | Counsel
212.735.2622 | stacey.cohen@skadden.com