American Bar Association
Section of Litigation
Committee on
Business Torts Litigation

Business Torts Journal (ISSN 1549-2923) is published quarterly by the Committee on Business Torts Litigation, Section of Litigation, American Bar Association, 321 N. Clark Street, Chicago, IL 60654-7598. The views expressed within do not necessarily reflect the views of the American Bar Association, the Section of Litigation, or the Committee on Business Torts Litigation.

www.abanet.org/litigation/committees/businesstorts

Business Torts Journal

Trade Secrets Issue

VOL. 18 NUMBER 1 ■ FALL 2010

RICO and the Theft of Trade Secrets

By Ashish S. Joshi

According to a recent study, there has been exponential growth in the theft of trade secrets.[1] Another study reveals that nearly 60 percent of employees who quit a job or are asked to leave are stealing company data.[2] Among those who took proprietary company data from their former employers, email was the most frequently stolen, followed by nonfinancial business information, customer contact lists, employee records, and financial information.[3] With this growth in the theft of trade secrets, it is no surprise that litigation in this area has increased as well. The Uniform Trade Secrets Act (UTSA) as adopted by various states is the most common tool used by litigators to combat the theft of trade secrets. The UTSA imposes civil liability for the misappropriation of trade secrets and creates a private cause of action for the victim. Remedies for misappropriation of trade secrets under the act include injunctions, damages such as exemplary damages, and, in cases of bad faith or willful and malicious misappropriation, reasonable attorney fees. Another seldom-used tool in a litigator's toolbox for theft of trade secrets litigation that is being utilized more and more is the Racketeer Influenced and Corrupt Organizations Act (RICO).

RICO was originally enacted to combat the infiltration of legitimate businesses by organized criminals.[4] By providing a broad federal structure for imposing criminal and civil liability on a wide range of conduct, RICO has succeeded in reaching illegal activity that is beyond the scope of other statutes. Though primarily designed as a weapon against organized crime, RICO's application has not been limited to the "archetypical, intimidating mobster."[5] RICO's provision for treble damages in civil cases has made its use more attractive and creative. The statute has been used against legitimate businesses that have committed "offenses" that can be wedged into RICO's racketeering definition, ranging from union tactics to the theft of trade secrets.[6] In regard to data thieves, RICO, with its capacity to provide for treble damages and attorney fees, provides a significant advantage over traditional remedies such as the UTSA or the federal Computer Fraud and Abuse Act (CFAA).[7]

RICO Elements

To recover in a civil RICO action, a plaintiff must prove that there is a violation of the RICO statute, 18 U.S.C. § 1962; that there is an injury to the plaintiff's business or property; and that the RICO violation was the proximate cause of the

(Continued on page 14)

Inside This Issue

RICO and the Theft of Trade Secrets

(Continued from page 1)

injury.[8] To establish a violation of the RICO statute, a plaintiff must in turn prove the conduct of an enterprise through a pattern of racketeering activity.[9] While defendants usually contest every element of a RICO claim, the battle usually focuses on proper pleading of the last two prongs: the "pattern" of "racketeering activity."

Racketeering Activity

RICO imposes criminal and civil liability upon those who engage in "racketeering activity," or, as the Supreme Court put it, "prohibited activities."[10] Racketeering activity is defined as "any act or threat involving" specific state-law crimes, any "act" indictable under various enumerated federal statutes, and certain federal offenses.[11] Prohibited activities that apply to the theft of trade secrets are mail fraud, wire fraud, and interstate transportation and receipt of stolen property with a value of $5,000 or more.[12] Each prohibited activity is defined in the RICO statute as including, as a necessary element, proof of either "a pattern of racketeering activity" or the "collection of an unlawful debt."[13] Of the term "pattern," the statute says that it "requires at least two acts of racketeering activity" within a 10-year period.[14]

Pattern

A "pattern of racketeering activity" is an occurrence of at least two acts of racketeering activity, known as predicate acts and enumerated in the statute, within a period of 10 years.[15] Demonstrating a "pattern of racketeering activity" also requires showing "that the racketeering acts are related and that they amount to or pose a threat of continued criminal activity."[16] "[A]llegations cannot constitute a RICO 'pattern' unless they satisfy both the 'relatedness' and 'continuity' tests."[17] However, both tests depend heavily on the specific facts of each case.

The test of relatedness is satisfied if the acts at issue "have the same or similar purposes, results, participants, victims, or methods of commissions, or otherwise are interrelated by distinguishing characteristics and are not isolated events."[18] Relatedness among the predicate acts for theft of trade secrets can be shown if the object was to steal the trade secrets for the purpose of using the victim's data for use by a competitor.[19]

In addition to satisfying the relatedness requirement, a RICO plaintiff must also satisfy the continuity requirement. Continuity signifies either a closed period of repeated conduct, i.e., "a series of related predicates extending over a substantial period of time," or "past conduct that *by its nature* projects into the future with a threat of repetition."[20]

Typically, the theft of trade secrets does not remain concealed for a long time; it is generally discovered shortly after it occurs. Accordingly, establishing close-ended continuity—conduct extending over substantial period of time—may not be feasible in the majority of circumstances, and all a RICO plaintiff is left with is to prove open-ended continuity through "past criminal conduct that by its nature projects into the future with a threat of repetition."[21]

In this circumstance, a RICO action for theft of trade secrets can be premised on the ground that the *past* theft poses a *future* threat of continuing criminal activity wherein the defendants will continue to use the stolen trade secrets. An argument can be made that there is a threat of continued activity because the defendants are continuing to use plaintiff's trade secrets. In addition, one can argue that not only did the defendants steal the plaintiff's trade secrets, but also the defendants threaten to commit additional predicate acts through their utilization of the stolen trade secrets.[22]

Open-Ended Continuity: *Gould* and *General Motors*

In *Gould*,[23] the plaintiff alleged that, prior to leaving its employment, its former employee copied and removed proprietary information that included trade secrets involving the manufacture of copper foil. The employee thereafter sold these trade secrets to two different companies who then proceeded to create a joint venture to construct a copper foil plant. The plaintiff brought a RICO claim against the two companies that received the stolen trade secrets from its former employee. In finding that the plaintiff sufficiently alleged a RICO claim, the *Gould* court, relying on the U.S. Supreme Court's decision in *H.J. Inc. v. Northwestern Bell Telephone Co.*,[24] noted that there was a threat of continued activity because the defendants would be continuing to use the plaintiff's trade secrets:[25]

> . . . there are allegations of a threat of continued activity . . . This joint venture allegedly will be using Gould trade secrets and, as this joint venture is constructed and operated, there will be an alleged continuing misappropriation of trade secrets that will continue to harm Gould. This certainly qualifies as a threat of continued wrongdoing as defined by H.J., Inc.[26]

Similar rationale prevailed in *General Motors Corp*.[27] General Motors (GM) alleged that its former employees secretly communicated with Volkswagen AG (VW) to leave GM and join VW. The employees agreed to bring confidential business plans and trade secret information with them that included listings of GM components by worldwide suppliers, price, terms, conditions, strategic purchasing models, and delivery schedules. The employees left GM with "20 cartons of stolen documents"[28] and joined VW, where they were paid significantly higher salaries. GM sued its former employees and VW for

RICO violations and other claims in a federal court in Michigan. GM alleged that the defendants' actions caused the company enormous damage. Given the fact that GM and VW were the two largest car sellers in Western Europe, VW's alleged use of GM's trade secrets enabled it to "reduce its costs substantially and to increase its market share."[29]

The flaw in *Minitab*, and certain of the cases upon which it relied, is that it improperly melds the separate acts of theft and subsequent use of the trade secrets into a single act.

The court agreed with GM's assertion that the allegations of the theft of trade secrets and their *threatened use* by VW were sufficient to allege an open-ended continuity. The court rejected VW's argument that each successive use of a trade secret did not constitute a new predicate act of theft and therefore subsequent use did not serve to continue a RICO scheme:

> When the Supreme Court spoke of the threat of repetition, it was referring to the threat of repeated *victimization* . . . not merely the retention of the ill-gotten fruits of previous crimes . . . The thief who steals $100 and then spends it a dollar at a time has victimized the owner only once, at the time the theft occurs. But the thief who steals a trade secret victimizes the owner every time the trade secret is used because the owner suffers a new loss with each use of the secret. . . . Moreover, although the predicate acts constituting the original theft of trade secrets do not threaten to be repeated, a fair and warranted inference to be drawn from the complaint is that the predicate acts of wire fraud, witness tampering, travel to aid racketeering, and transportation of stolen goods threaten to be repeated as the Defendants make use of the stolen trade secrets.[30]

Theft vs. Use: Threat of Future Activity

Not all courts have agreed with the *Gould* and *General Motors* rulings that a threat of continued criminal activity can be inferred from a theft of trade secrets. A federal district court in the Middle District of Pennsylvania refused to follow the rationale laid down in the *Gould* and *General Motors* decisions.[31] The *Minitab* court cleaved the theft of trade secrets from its subsequent use and refused to see the subsequent use of the trade secret as sufficient to establish a continued threat of future activity:

> . . . [W]e believe that using trade secrets is quite different from the initial act of stealing them. In fact, we believe that the theft of trade secrets necessarily implies that they will be used. Therefore, under plaintiff's theory, every misappropriation of trade secrets could result in a RICO claim. This would surely expand the scope of the statute beyond what it was intended to reach.[32]

The principal flaw in *Minitab*, and certain of the cases upon which it relied, is that it improperly melds the separate acts of theft and subsequent use of the trade secrets into a single act.[33] The theft of an item and its subsequent use and/or possession have been universally recognized as distinct criminal acts, with the theft a precondition for use and/or possession. For example, the Economic Espionage Act makes theft and possession separate crimes. RICO predicate 2314 applies to the theft of data, while 2315 applies to the possession of the stolen data.[34]

While the theft of trade secrets may well be the gravamen of a RICO action, the subsequent use of stolen trade secrets poses a serious risk of repeated victimization. In *General Motors*, GM complained of a continuing threat of injury—that VW continued to use GM's trade secrets "to reduce [VW's] costs substantially and to increase its market share"[35] to GM's detriment. Not only was GM injured when its trade secrets were misappropriated, but also every subsequent use of those trade secrets further victimized GM, because it suffered a new loss with each use.

The *Minitab* court appears to have adopted the oft-cited logic that:

> When a thief steals $100, the law does not hold him to a new theft each time he spends one of those dollars. The same is true of the [trade secrets] . . . Its subsequent and varied uses . . . would not constitute new offenses but would go only to the issue of damages.[36]

The court clarified that "if plaintiff's complaint were to allege that defendants would continue to steal plaintiff's trade secrets, as opposed to use those which have already been stolen, then there may well be a threat of continuity."[37] In other words, the court simply saw use of stolen trade secrets as "the retention of the ill-gotten fruits of previous crime."[38] Unless a plaintiff alleged that a defendant would continue to steal the plaintiff's trade secrets, there would be no RICO liability for any subsequent use of stolen trade secrets. This overly simplistic reasoning does not do justice to the novel nature of trade secrets that derive "independent economic value, actual or potential, from not being generally known."[39] The value of a trade secret arises specifically from the fact that it is not generally known.

The value is not just the worth of the information itself. By the same token, the benefits derived from a theft of trade secrets are primarily the benefits derived from its *use* and the cost avoided in independently developing such information.

A trade secret is confidential and protected information that is not only crucial to the success of its owner but also beneficial to a rival operating in the same market as its owner. In other words, unlike a thief who continues to spend dollars out of the total $100 that he stole, each successive use of a misappropriated trade secret not only benefits the person who stole it but also damages the aggrieved owner. Use of misappropriated trade secrets has real-world implications.

The theft of trade secrets and other proprietary information that businesses develop after spending fortunes and devoting considerable resources to research and development is not similar to other garden-variety theft. The *General Motors* court hit the nail on the head when, distinguishing the retention of the ill-gotten fruits of a theft from the threat of repeated victimization, it held that "the thief who steals a trade secret victimizes the owner *every time* the trade secret is used because the owner suffers a *new loss* with each use of the secret."[40] The requirement of open-ended scheme was satisfied because VW threatened "to commit predicate acts through their *utilization* of the stolen trade secrets."[41] Every use of GM's trade secrets was a threat "of continued activity because [VW] would be continuing to use [GM's] trade secrets."[42]

Stolen trade secrets can be used to penetrate new markets, reduce a competitor's costs, increase a competitor's market share, and do a million different things that would have otherwise required a serious expenditure of resources if done in a legal and legitimate manner.[43] Every use of misappropriated trade secrets continues to harm the victim of the theft. Moreover, although the predicate acts constituting the original theft of trade secrets do not threaten to be repeated, other ancillary predicate acts such as wire fraud, witness tampering,[44] travel to aid racketeering, and transportation of stolen goods threaten to be repeated as the trade secrets are used.[45]

Further, the *Minitab* court's reasoning that "every misappropriation of trade secrets could result in a RICO claim" and therefore would "surely expand the scope of the statute beyond what it was intended to reach," is misplaced.[46] First, the Supreme Court has "repeatedly refused to adopt narrowing constructions of RICO to make it conform to a preconceived notion of what Congress intended to proscribe."[47] Second, the Supreme Court has also held that the fact that RICO may be applied to situations not expressly anticipated by Congress does not demonstrate ambiguity. "It demonstrates breadth."[48]

Also, courts have explained that damages for RICO claims for the theft of trade secrets can be measured by the victim's loss or by the wrongdoer's profits.[49] Further, lost profits are recoverable under RICO as well. This fits in with the reasoning of the *General Motors* court. "Open-ended" continuity occurs where the past conduct projects into the future *by its very nature* with a threat of repetition.[50] Because of the threat of the use of stolen trade secrets, open-ended continuity should be established in these cases.

Conclusion

Given the split in the federal courts, it is essential to check the appropriate circuit law before filing a RICO action predicated on the theft of trade secrets. The *Minitab* opinion and other cases from the Third Circuit essentially foreclose a RICO action unless a plaintiff alleges a closed-ended continuity of predicate acts that have occurred over a substantial period of time. If not, then a plaintiff will have to demonstrate open-ended continuity by alleging that the defendants would continue to steal the plaintiff's trade secrets unless restrained. *General Motors* and other cases from the Sixth Circuit, however, allow a plaintiff to demonstrate open-ended continuity by showing use of stolen trade secrets. A plaintiff need not demonstrate that defendants would continue to steal trade secrets—a tough, if not unrealistic, burden to carry.

Each successive use of a misappropriated trade secret not only benefits the person who stole it but also damages the aggrieved owner.

Overall, it is crucial in a RICO complaint predicated on the theft of trade secrets to allege in as much factual detail as possible the circumstances demonstrating the theft of trade secrets, continued and/or threatened use of the stolen trade secrets and the resulting victimization, how the theft will lead to the commission of further criminal activity, and the future criminal activity—the predicate acts—as separate and distinct violations. ■

Ashish S. Joshi is a shareholder attorney at Lorandos & Associates in Ann Arbor, Michigan.

Endnotes

1. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291 (2010).
2. Brian Krebs, *Data Theft Common by Departing Employees*, Wash. Post, Feb. 26, 2009.
3. *Id.*
4. Melvin I. Urofsky, *RICO*, The Oxford Companion To American Law 706 (Kermit Hall et al. eds., 2002).

5. Sedima SPRL v. Imrex Co. Inc., 473 U.S. 479, 498 (1985).
6. Kris Maher, *Firms Use RICO to Fight Union Tactics*, Wall St. J., Dec. 10, 2007, *available at* http://online.wsj.com/article/SB119725268618018954.html?mod=googlenews_wsj.
7. Nick Akerman, *RICO and Data Thieves*, Nat'l L. J. 12 (June 9, 2008).
8. Holmes v. Sec. Inv. Prot. Corp., 503 U.S. 258, 265-68 (1992).
9. Sedima, 473 U.S. at 496.
10. H.J. Inc. v. Nw. Bell. Tel. Co., 492 U.S. 229, 232 (1989).
11. 18 U.S.C. § 1961(1) (1994).
12. 18 U.S.C. §§ 1341, 1343, 2314, 2315.
13. *Id.*
14. 18 U.S.C. § 1961(5) (1994).
15. Sedima SPRL v. Imrex Co., 473 U.S. 479, 496 n.14 (1985).
16. H.J. Inc. v. Nw. Bell. Tel. Co., 492 U.S. 229, 239 (1989).
17. Kehr Packages, Inc. v. Fidelcor, Inc., 926 F.2d 1406, 1412 (3d Cir.1991).
18. H.J. Inc., 492 U.S. at 240.
19. General Motors Corp. v. Ignacio Lopez de Arriortua, 948 F. Supp. 670, 677-78 (E.D. Mich. 1996).
20. H.J. Inc., 492 U.S. at 241 (emphasis added).
21. United States v. Browne, 505 F.3d 1229, 1259 (11th Cir. 2007) (citing H.J. Inc., 492 U.S at 241).
22. *See, e.g.*, General Motors Corp., 948 F. Supp. at 678 (citing Gould, Inc. v. Mitsui Mining & Smelting Co., 750 F. Supp. 838 (N.D. Ohio 1990)).
23. Gould, 750 F. Supp. 838.
24. H.J. Inc., 492 U.S. 229.
25. Gould, 750 F. Supp. at 842.
26. *Id.*
27. 948 F. Supp. at 678–79.
28. *Id.* at 674.
29. General Motors Corp., *supra* at 675.
30. *Id.* at 678-679
31. Binary Semantics Ltd. v. Minitab Inc., No. 4:07-CV-1750, 2008 WL 763575, at *4 (M.D. Pa. March 20, 2008).
32. *Id.*
33. Nick Akerman, *RICO and Data Thieves*, The National Law Journal, June 9, 2008.
34. *Id.*
35. General Motors Corp., *supra* at 675.
36. Management Computer Services, Inc. v. Hawkins, Ash, Baptie & Co., 883 F.2d 48, 51 (7th Cir. 1989).
37. Binary Semantics Ltd., *supra*.
38. Gotham Print, Inc. v. American Speedy Printing Centers, Inc., 863 F.Supp. 447, 460 (E.D. Mich. 1994).
39. Uniform Trade Secrets Act, § 1.
40. General Motors, *supra,* at 679 (emphasis added).
41. *Id* at 678 (E.D.Mich., 1996) (emphasis added).
42. *Id.*
43. *Id.* at 675.
44. Witness tampering under 18 U.S.C. § 1512 includes misleading conduct with intent to cause a person to withhold testimony or a document as well as alteration of documents. Thus, making false statements regarding whether someone has stolen trade secrets or conducting an internal "investigation" that is designed to mislead investigators or others in investigating a theft of trade secrets constitutes witness tampering. *See* General Motors Corp. v. Ignacio Lopez de Arriortua, 948 F.Supp. 670, 678 (E.D.Mich., 1996).
45. General Motors, *supra*, at 678; *also see* Gould, Inc. v. Mitsui Mining & Smelting Co., 750 F.Supp. 838 (N.D. Ohio 1990).
46. Binary Semantics Ltd., *supra*.
47. Bridge v. Phoenix Bond & Indemnity Co., 128 S.Ct 2131, 2145, 170 L.Ed.2d 1012 (2008).
48. Boyle v. United States, 129 S.Ct. 2237, 2247, 173 L.Ed.2d 1265 (2009) citing Sedima SPRL v. Imrex Co. Inc., 473 U.S. 479, 498 (1985).
49. General Environmental Science Corp. v. Horsfall, 800 F.Supp. 1497, 1503 (N.D.Ohio 1992), *aff'd in part, vacated in part on different grounds*, 25 F.3d 1048 (6th Cir.1994).
50. H.J.Inc., *supra* at 242.