THE NATIONAL
LAW JOURNAL
DAILY UPDATES ON WWW.NLJ.COM | THE WEEKLY NEWSPAPER FOR THE LEGAL PROFESSION | MONDAY, JUNE 9, 2008 | ALM

BUSINESS INFORMATION

RICO and Data Thieves

By Nick Akerman

THE CIVIL REMEDY in the Racketeer Influenced and Corrupt Organizations (RICO) statute, 18 U.S.C. 1961, et. seq., is not limited to the "archetypal, intimidating mobster." *Sedima SPRL v. Imrex Co. Inc.*, 473 U.S. 479, 498 (1985). There is no reason why RICO cannot apply to data thieves. RICO provides a significant remedial advantage over traditional remedies such as the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030(g), which directly outlaws the theft of data, and, like RICO, provides for a civil remedy. The CFAA, however, is limited to compensatory damages, whereas RICO provides for treble damages and attorney fees. 18 U.S.C. 1964(c). This article will review the elements of a civil RICO action as they apply to data theft and how to frame a successful RICO suit predicated on data theft.

To allege and prove civil RICO, a plaintiff "must show that he was injured by defendants' (1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *Sedima SPRL*, 473 U.S. at 496. The threshold issue is whether the data thief was acting through a RICO "enterprise." The statute defines enterprise as "any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity." 18 U.S.C. 1961(4). The enterprise and the defendant cannot be the same.

There must also be "some distinctness between the RICO defendant and the RICO enterprise." *Cedric Kushner Promotions Ltd. v. King*, 533 U.S. 158, 163 (2001). In *King*, for example, the court held that "the need for two distinct entities is satisfied" when there is an individual defendant and the RICO enterprise is his wholly owned corporation. In the context of data theft the "enterprise" can be the victim company, the competing company, individuals that used the stolen data or an association-in-fact consisting of entities or individuals who participated in or benefited from the theft.

'Racketeering activity' can include acts of data theft

The element of "racketeering activity" is defined by the statute to include a specified list of state and federal crimes upon which the RICO action may be predicated. 18 U.S.C. 1961(1). A RICO plaintiff must allege and prove by a preponderance of the evidence that the defendant committed the criminal acts underlying the RICO count. The criminal acts that apply to data theft are mail fraud, 18 U.S.C. 1341; wire fraud, 18 U.S.C. 1343; and interstate transportation and receipt of stolen property, the value of which is $5,000 or more, 18 U.S.C. 2314, 2315.

The mail and wire fraud statutes outlaw schemes to defraud, the object of which is to steal property. That the property is intangible computer data "does not make it any less 'property' protected by the mail and wire fraud statutes." *Carpenter v. U.S.*, 484 U.S. 19, 26 (1987). The use of the mails or interstate wires, such as e-mailing from state to state in furtherance of the scheme, provides federal jurisdiction for the crime.

In contrast to the mail and wire fraud statutes, the courts disagree on whether intangible computer data can be the property stolen or received in violation of §§ 2314 and 2315. Relying on *Dowling v. U.S.*, 473 U.S. 207 (1985), which refused to apply § 2314 to bootlegged movies, *U.S. v. Brown*, 925 F.2d 1301, 1307-8 (10th Cir. 1991), held that computer information "is an intangible intellectual property" and is not "goods, wares or merchandise" within the meaning of §§ 2314 and 2315.

An exception exists, however, when, "there has been 'some tangible item taken, however insignificant or valueless, it may be.' " *U.S. v. Martin*, 228 F.3d 1, 14-15 (1st Cir. 2000). Thus, if an employee steals data worth $5,000 or more from the company computers and also steals the disk upon which he stores the stolen data and takes the disk to another state, the theft violates § 2314.

The 2d U.S. Circuit Court of Appeals rejects this distinction between tangible and intangible property and applies the statutes to the theft of computer data. For example, in *U.S. v. Farraj*, 142 F. Supp. 2d 484, 489 (S.D.N.Y. 2001), the court upheld the validity of a § 2314 charge when a paralegal e-mailed across state lines his employer law firm's con-

Nick Akerman *is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data.*

fidential and proprietary trial plan. Because of this divergence in law, it is essential to check the appropriate circuit law before filing a RICO action predicated on violations of §§ 2314 or 2315.

Plaintiffs must also satisfy the 'pattern' requirement

A RICO plaintiff must also allege and prove that the criminal predicate acts constitute a "pattern." The U.S. Supreme Court has defined "pattern" as more than simply the statutory requirement of "at least two acts of racketeering activity...within ten years." 18 U.S.C. 1961(5). Based on the legislative history, the Supreme Court requires that the criminal acts predicating the RICO violation be "related," and that "they amount to or pose a threat of continued criminal activity." *H.J. Inc. v. Northwestern Bell Tel. Co.*, 492 U.S. 229, 239 (1989).

The criminal acts are related if they "have the same or similar purposes, results, participants, victims, or methods of commission, or otherwise are interrelated by distinguishing characteristics and are not isolated events." *H.J. Inc. v. Northwestern Bell*, 492 U.S. at 240. Relatedness among the predicate acts for stealing computer data can be shown if the object was to steal data from one or more victims for the purpose of using the victims' data in competition or perpetrating identity theft. See, e.g., *General Motors Corp. v. Arriortua*, 948 F. Supp. 670, 673, 677-78 (E.D. Mich. 1996) (predicate crimes all related to theft of trade secrets, including those on computer disks from the same victim for use by a competitor).

In addition to the requirement that the criminal acts must be related, they must be continuous for there to be a valid RICO "pattern." "Continuity is both a closed- and open-ended concept, referring either to a closed period of repeated conduct, or to past conduct that by its nature projects into the future with a threat of repetition." *H.J. Inc.*, 492 U.S. at 241. Continuity over a closed period must constitute related illegal activity over "a substantial period of time." Id. at 242. While there is no bright-line test for determining precisely what period of time is "substantial," ordinarily the predicate acts must have been committed for at least two years. *Spool v. World Child Intern. Adoption Agency*, 520 F.3d 178, 184 (2d Cir. 2008).

'Minitab': Plaintiff failed to allege open-ended pattern

The classic data theft is usually not concealed for two years but is discovered shortly after it occurs. Given that practical reality, the most common method to prove a "pattern" relating to data theft is to show open-ended continuity through "past criminal conduct that by its nature projects into the future with a threat of repetition." *U.S. v. Browne*, 505 F.3d 1229, 1259 (11th Cir. 2007). There is a disagreement among the federal courts as to whether a threat of continuing criminal activity can be inferred from a theft of data. A recent federal district court case, *Binary Semantics Ltd. v. Minitab Inc.*, No. 4:07-CV-1750, 2008 WL 763575, at *4 (M.D. Pa. March 20, 2008), dismissed a RICO count based on the theft of trade secret data, holding that the plaintiff failed to allege an open-ended pattern.

There is no reason why RICO, which provides a notable remedial advantage over other remedies, cannot apply to data thieves.

The court refused to follow *General Motors*, 948 F. Supp. at 678, and *Gould Inc. v. Mitsui Mining & Smelting Co.*, 750 F. Supp. 838, 842 (N.D. Ohio 1990), both of which upheld civil RICO counts on the basis that the theft of trade secrets does pose a threat of continuing criminal activity to use the stolen trade secrets. The *Minitab* decision was premised on the court's belief "that the theft of trade secrets necessarily implies that they will be used" and relied on four district court cases that "reached conclusions contrary to *General Motors* and *Gould*." *Minitab*, 2008 WL 763575, at *4.

Theft and use are distinct criminal acts

The principal flaw in *Minitab*, and certain of the cases upon which it relies, is that it improperly melds the theft and use of the trade secrets into a single crime, when theft and use are universally recognized as distinct criminal acts with the theft a precondition for use. For example, the Economic Espionage Act, 18 U.S.C. 1831(a)(1)(3), while not a RICO predicate, makes theft and possession separate crimes. This distinction also applies to a violation of the RICO predicates § 2314 for theft of data and a violation of § 2315 for possession of the stolen data. Indeed, "[w]hen 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" and "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." *General Motors*, 948 F. Supp. at 679.

That "threat of the unbridled continuation of the violation" supports a judicial finding of irreparable harm justifying the entry of a preliminary injunction. *John G. Bryant Co. Inc. v. Sling Testing and Repair Inc.*, 369 A.2d 1164, 1167 (Pa. 1977). Similarly, a thief who steals data to commit identity theft later victimizes each person whose identity he or she steals. Given the *Minitab* opinion, it is critical in a RICO count predicated on data theft to allege in as much factual detail as possible the circumstances demonstrating why the theft will likely lead to further criminal activity and victimization and to allege this future criminal activity as separate and distinct violations of the federal criminal law. NLJ