Trade Secret Misappropriation A Federal Crime

BY JAMES D. VELTROP OF AXINN, VELTROP & HARKRIDER

On October 11, 1996, President Clinton signed into law the Economic Espionage Act of 1996 (the "Act"), which for the first time made the misappropriation of trade secrets a federal crime. Trade secret misappropriation had heretofore been the near-exclusive province of state civil law,[1] usually in the form of the Uniform Trade Secrets Act ("UTSA") or a slightly modified variation thereof. The new law raises a host of as yet unanswered questions as to the scope of its application, the extent of its enforcement and the difference between civil and criminal trade secret misappropriation.

At least three major driving forces behind the passage of the Act can be identified. One is the growing recognition that the future of the American economy lies in technology, and growing outrage over the extensive involvement of foreign governments in industrial espionage. The new "Cold War" revolves around the battle for technology. A second is the onslaught of numerous well-publicized and notorious cases of international trade secrets misappropriation, including the Jose Lopez case, which was recently settled by General Motors but which is still the subject of criminal prosecution in Germany. A third is the burgeoning use of computers and the Internet to facilitate the theft and transmission of confidential databases and technology.

The Act is designed to address these concerns and equips prosecutors with international enforcement powers as well as broad standards of liability aimed at high-tech methods of theft. The Act is not, however, limited to these grand purposes. Rather, it applies equally to garden-variety domestic trade secrets disputes and now raises the spectre of criminal liability in many of these cases. Trade secret issues are a staple of corporate life, and are a very common type of litigation. Particularly given its infancy, the Act raises critical issues for counsel and their clients to consider in order to avoid criminal liability as well as to more adequately protect valuable trade secrets.

The Act adopts a broad definition of trade secrets that is similar to that found in UTSA, except that it is updated to reflect recent technological innovations. Trade secrets are defined as:

> 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 the public.

18 U.S.C. § 1839(3). Like UTSA, the definition of trade secrets under the Act is also likely to include a wide range of business and technical information not specifically mentioned, such as customer lists and methods of doing business.

Misappropriation, or "conversion," of trade secrets is also quite broadly defined to cover practically all conceivable unauthorized use or acquisition of trade secrets. Some of the examples specifically cited in the Act include stealing, concealing, taking by fraud or deception, copying, duplicating, sketching, downloading, altering, destroying, transmitting, sending, communicating or conveying a trade secret. *Id.* §§ 1831(a)(1)-(2); 1832(a)(1)-(2). Transmitting stolen information over the Internet obviously falls within these restrictions. Where the initial acquisition of the trade secret is authorized, e.g., pursuant to a confidentiality agreement, the Act will presumably be interpreted, consistent with UTSA, to find misappropriation if, and only if, some unauthorized use or dissemination occurs. Like UTSA, the Act also applies to the purchase or receipt of trade secrets while knowing them to have been misappropriated. *Id.* §§ 1831(a)(3); 1832(a)(3).

Unlike UTSA, the Act does apply both to the *attempted* misappropriation of trade secrets as well as to the formation of a *conspiracy* to misappropriate trade secrets. *Id.* §§ 1831(a)(4)- (a)(5), (b); 1832(a)(4)-(a)(5). (In the latter case, at least one member of the conspiracy must have acted to further the ends of the conspiracy.) In other words, an UTSA civil action will lie only for successful and completed acts of misappropriation, whereas a federal criminal action will lie for failed attempts, as well as for belonging to a conspiracy that has taken one step towards the end of misappropriation.

The Act's definition of the crime of trade secret misappropriation, then, is at least as broad as UTSA's definition of trade secret misappropriation and arguably broader in certain respects. At the same time, the Act provides for harsh criminal penalties that in many circumstances are far more substantial than the civil remedies provided by UTSA.

A civil plaintiff under UTSA is typically awarded single damages for harm actually caused by the defendant and proved by the plaintiff. Injunctive relief is typically limited to the time it would have taken the defendant to derive the trade secrets independently. Courts also have been willing to enjoin individuals from certain employment that would lead to the inevitable misappropriation of trade secrets learned from a prior employer. A plaintiff who is able to prove that the misappropriation was willful and malicious may, in the discretion of the court, be awarded punitive damages in an amount not exceeding twice the amount of actual damages, as well as reasonable attorneys' fees.

The criminal penalties provided by the Act, which apply in addition to these civil penalties, are extremely harsh. A person who violates the Act can be fined up to $500,000 and imprisoned for up to 10 years. A corporation or other organization can be fined up to $5 million. *Id.* § 1832(a), (b). Moreover, if the misappropriation knowingly benefits a foreign government or an instrumentality or agent thereof, the maximum individual prison sentence is increased to 15 years and the maximum fine for a corporation or other organization is increased to $10 million. *Id.* § 1831(a), (b). Significantly, the Act also provides for the criminal forfeiture to the United States of any property gained from the misappropriation, or used in an attempt to effect the misappropriation, e.g., a computer used to transmit stolen trade secrets over the Internet. *Id.* § 1834. Federal prosecutors also are empowered to institute civil actions in federal district court to enjoin violations of the Act. *Id.* § 1836.

However, the necessary elements of the federal crime of trade secret misappropriation, as well as the penalties for committing this crime, cannot be understood from the face of the statute. As to penalties, the Act merely sets forth the maximum penalties available, which are unlikely to be imposed on first time offenders. The actual sentence will be the product of a U.S. District Court judge's analysis of the multiple factors set forth in the Federal Sentencing Guidelines. Under these Guidelines, a base offense level is defined according to the nature of the crime, and this level is then adjusted according to the Court's assessment of several specified aggravating or mitigating circumstances. As many white-collar antitrust defendants have found out, it would appear unlikely that an individual convicted of trade secrets misappropriation would avoid significant fines and jail time.

As to the crime of misappropriation itself, there are several significant difference between UTSA and the Act that are not apparent from the face of the Act. The first and most obvious is that civil UTSA plaintiffs must prove their case by a preponderance of the evidence whereas criminal prosecutors must establish guilt beyond a reasonable doubt. This difference in legal standards will be significant in many trade secrets cases, given that they typically involve circumstantial evidence and numerous ambiguous questions of fact and law.

An equally significant difference is that the Act, like other criminal statutes, requires proof of intent or knowledge. Moreover, the due process clause of the U.S. Constitution requires that criminal statutes must give defendants adequate notice as to what constitutes a violation. These standards could be rather difficult to meet in cases involving technical and circumstantial issues and substantial disagreement over what constitutes a trade secret in the first place. Nonetheless, intent has been found in numerous civil cases in which exemplary damages were awarded for willful and malicious behavior. At a minimum, a substantial portion of these types of future cases could be possible candidates for prosecution under the Act. One means for clients to minimize this risk is to seek an opinion of counsel in order to negate possible inferences of intent to misappropriate.

Perhaps the most significant difference, at least from a practical perspective, is the exercise of prosecutorial discretion. Misappropriation cases raise a number of private considerations that are more appropriately resolved in civil litigation, as well as a number of gray issues that are simply inappropriate for criminal prosecution. Moreover, the sheer number of misappropriation cases nationwide would severely tax the resources of federal prosecutors. Nonetheless, the literal terms of the Act would appear to apply, at the outset, to a number of misappropriation cases, and criminal complaints may be the only practical remedy for smaller companies, particularly in international cases. Federal prosecutors will have to exercise appreciable restraint in order to strike a workable compromise between numerous conflicting concerns. The Department of Justice has undertaken to implement regulations that, for a period of five years, would permit the pursuit of an indictment only with the prior approval of the Assistant Attorney General for the Criminal Division or a higher official. *See* Cong. Rec. S12214 (Oct. 2, 1996).

Restraint is required because many misappropriation cases, particularly potential criminal actions, exact significant social costs as well. In civil cases, for example, the courts have struggled to strike a balance between, on the one hand, the need to protect trade secrets while, on the other hand, preserving an employee's right to seek alternative employment, or a competitor's right, for the good of consumers and the economy, to engage in aggressive competition free of unreasonable restraints. Excessive criminal actions could impose a particularly chilling effect on the high-tech industry, which thrives on the exchange of ideas and is characterized by frequent employee turnover. Companies will have to be particularly sensitive to issues raised by the hiring of senior or technical employees from competitors, or by the formation of strategic alliances.

Thus, another significant area of corporate law has been criminalized. If it is not already, intellectual property should now be a part of every corporate compliance program, and corporate executives be advised of the potentially criminal implications of trade secret issues. For companies that have not yet implemented corporate compliance programs, the Act is but one more reason for doing so. Criminal issues such as those raised by the Act must be addressed in a proactive manner, and effective compliance programs avoid problems and minimize penalties should problems nonetheless arise. The Act also provides a potentially powerful new weapon for companies to protect against trade secret misappropriation. IPT

ENDNOTES

1. California passed a similar law earlier in 1996. Other states have laws making intellectual property theft a misdemeanor, but these laws are rarely enforced. Congress is also examining the need for a federal civil cause of action for trade secrets misappropriation. See Cong. Rec. S12208 (October 2, 1996).