REPRINT FINANCIER WORLDWIDE

JUNE 2017

FINANCIER WORLDWIDE corporatefinanceintelligence

INTELLECTUAL PROPERTY

Trade secret theft in the digital age

PETER S. SELVIN

TROYGOULD PC

In the pre-internet age, instances of trade secret theft were typically tied to specific geographic locations and specific physical items. For example, an employee operating from his employer's physical location misappropriates a paper customer list or the plans and specifications for a product. Or a business partner, entrusted with physical materials that are proprietary and confidential, shares or disseminates those materials in an unauthorised manner.

But in the digital age, physical presence or proximity is no longer a necessary condition for trade secret theft. For example, cyber criminals and hackers operating outside the physical boundaries of the country where a computer server is located may remotely infiltrate that computer system and obtain protected trade secrets. In addition, with the advent of a highly mobile workforce, trade secrets may reside inside the brains of a company's former employees or business partners, and those individuals may themselves relocate to jurisdictions outside the company's physical location.

Peter S. Selvin is an attorney at TroyGould PC. He can be contacted on +1 (310) 789 1230 or by email: pselvin@troygould.com.

© 2017 Financier Worldwide Limited.
Permission to use this reprint has been granted by the publisher.

In keeping with these changes, the US Congress last year passed the Defend Trade Secrets Act (DTSA), which essentially federalises US trade secret law. This statute may be of particular interest to companies operating outside the US because it specifically targets trade secrets used in, or intended for use in, interstate or foreign commerce. This means that companies operating with US counterparties face an additional issue of risk management concern.

The passage of DTSA may have been prompted by several high-profile misappropriation cases, including DuPont v. Kolon Industries, in which DuPont obtained a $1bn jury verdict arising out of Kolon's alleged misappropriation of DuPont's kevlar technology; and TianRui Group Co., Ltd. v. ITC, where the court held that the US International Trade Commission had authority to restrict the importation of goods into the US that were produced through the misappropriation of trade secrets, even if the acts of misappropriation occurred abroad.

The emphasis on conduct outside the US is reflected throughout the statute. For example, Section 4 of the statute, entitled 'Report on Theft of Trade Secrets Occurring Abroad', charges the US attorney general with periodic reporting to Congress about "the scope and breadth of the theft of trade secrets of United States companies occurring outside of the United States". Section 5 of the statute recites Congress' conviction that "trade secret theft occurs in the United States and around the world" and that "wherever it occurs, [such conduct] harms the companies that own the trade secrets and the employees of the companies".

Consistent with these underlying policies, the application of the statute is very broad. Thus, the theft of trade secrets is actionable in US courts so long as the secrets are "related to" goods or services sold, or intended to be sold, in the US. This is a very low threshold. Thus, if managers from a Dutch company solicit employees of a Czech company to misappropriate trade secrets from the Czech company relating to goods or services sold in the US, the Czech company may presumably sue both its employees and the Dutch company in the US, thereby securing the advantage of US-style discovery and the ex parte seizure and other enumerated remedies available under the statute.

Companies doing business, or contemplating doing business, with US counterparties should also be aware that DTSA requires that a whistleblower immunity provision be included in all confidentiality agreements with employees, contractors or consultants. Importantly, the statute provides that the failure to include this immunity provision in such contracts may result in the forfeiture of the right to recover attorneys' fees under the statute.

The criminal counterpart to DTSA is the Economic Espionage Act (EEA). Highlighting the international dimension to trade secret theft, Section 7 of the EEA, provides that the statute applies to conduct occurring outside the US if, among other circumstances, "an act in furtherance of the offense was committed in the United States". This section was not modified or affected by the enactment of the DTSA.

The potential extraterritorial application of DTSA is also underscored by the fact that the statute amends the definition of "racketeering activity" under the US

© 2017 Financier Worldwide Limited.
Permission to use this reprint has been granted by the publisher.

RICO statute to include violations of the EEA. This means that trade secret theft amounting to a criminal violation under the EEA now qualifies as a "predicate offence" for purposes of the federal RICO statute. As a result, trade secret theft can now serve as the basis of a civil RICO claim under applicable US law even if the perpetrators are domiciled outside the US.

The advent of DTSA means that companies based outside the US – but who are dealing with US counterparties – need to become aware of what the US courts consider to be protectable trade secrets. In addition, those companies would also be well-advised to conduct periodic audits to determine whether they are using illicitly transferred US technology in their operations. Given the global scope of trade secret theft, such measures will mitigate the risk that companies based outside the US could be obliged to respond to US litigation. ■

© 2017 Financier Worldwide Limited.
Permission to use this reprint has been granted by the publisher.