Feeling the pinch

The conviction of a Goldman Sachs programmer for stealing trade secrets has profound implications for US companies' IP, argue Baker Hostetler's Jonathan B New and Christy Nixon

The protection of proprietary data and processes from misappropriation by departing employees remains one of the most challenging areas of employment and criminal law. With the fortunes of entire businesses rising and falling on proprietary information, especially as trading on Wall Street becomes more automated, the ability of established businesses to protect their proprietary models, and for new firms to recruit and grow free of claims of trade secrets theft, are becoming an ever-more critical challenge for businesses and the lawyers who counsel them.

Of late, the Department of Justice (the “DOJ”) has placed an emphasis on investigating and prosecuting intellectual property (“IP”) offences. In February 2010, Attorney General Eric Holder announced the creation of the IP Task Force as part of the DOJ’s initiative to combat the growing number of domestic and international IP crimes. As of September 2011, the FBI had 499 pending IP crime investigations, 100 of which concerned trade secrets theft. Also in September 2011, the DOJ announced its award of $4.9m to state and local law enforcement agencies for education, deterrence, enforcement and evidence gathering to prosecute IP crimes in coordination with federal efforts.

While the DOJ’s initiative offers corporations another tool to protect their proprietary information, a recent Second Circuit decision alters the analysis of whether a company should make a criminal referral or proceed with traditional civil avenues of relief. More than ever, corporate counsel should adopt certain best practices as preventive measures with an eye toward the legal options available in responding to a suspected trade secrets theft.

Federal law criminalises theft of trade secrets

The Economic Espionage Act of 1996 (the “EEA”), criminalises two types of trade secret misappropriation: commercial economic espionage and foreign economic espionage. Conviction under both requires that the defendant knowingly misappropriated a trade secret. Misappropriation includes the possession, receipt, purchase, destruction, duplication or transmission of a stolen trade secret. A trade secret is any type of financial, business, scientific, technical, economic or engineering information derived independent economic value from not being generally known to the public and is the subject of the owner’s reasonable efforts to maintain its secrecy.

To commit foreign economic espionage, a defendant must intend to benefit, or know that the offence would benefit, a foreign government, instrumentality or agent. In contrast, for commercial economic espionage a defendant must intend to convert the trade secret to the economic benefit of someone other than the owner. Commercial economic espionage may lead to 10 years imprisonment and a fine on organisations up to $10m. Foreign economic espionage could lead to 15 years’ imprisonment and a fine on organisations up to $100m.

Prior to the enactment of the EEA, there was no federal criminal statute expressly criminalising theft of commercial trade secrets.

Prosecutors often had difficulty fitting trade secrets theft within the existing federal statutes. Congress enacted the EEA because it recognised that proprietary economic information (ie, intangible assets, such as production processes, bid estimates, production schedules, computer software and technology schematics) was increasingly important to the nation’s economy and could easily be stolen. It intended the EEA to punish all categories of trade secrets theft including “the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics.”

The Second Circuit’s surprising limit on the EEA

In a recent groundbreaking decision, however, the Second Circuit Court of Appeals limited prosecutors’ ability to pursue criminal charges for theft of trade secrets under the EEA. The Court reversed the jury conviction of former Goldman Sachs Group Inc (“Goldman Sachs”) programmer Sergey Aleynikov under, among other things, the EEA for transferring the proprietary computer source code from Goldman Sachs’ high-frequency trading program. The decision has dealt a significant setback to the DOJ’s recent effort to aggressively investigate and prosecute IP crimes. As a result, internal management practices and the civil remedies traditionally available to protect trade secrets are even more critical to businesses in highly competitive, proprietary trading and other technology-intensive markets.

On 18 March 2011, Aleynikov was sentenced to more than eight years of imprisonment after having been found guilty by a jury on 10 December 2010, for stealing the proprietary computer code for Goldman Sachs’ high-frequency trading platform and transferring it to a server in Germany, then downloading to his computer devices in New Jersey, and later bringing the computer devices with him to Illinois with the purpose of building a similar computer trading platform at another firm. Aleynikov was charged and convicted for violating, among other things, the EEA by downloading a trade secret “that is related to or included in a product that is produced for or placed in interstate or foreign commerce,” with the intent to convert such trade secret and to injure its owner, to the economic benefit of anyone under the owner. He appealed his conviction to the Second Circuit arguing, among other things, that his conduct did not constitute an offence under the EEA because he had not stolen trade secrets related to a product made for the purposes of interstate or international commerce.

On 17 February 2012, following oral argument held that same day, the Second Circuit issued a short order reversing Aleynikov’s conviction under the EEA – to the surprise of many – and indicated that an opinion would follow. Almost two months later, the Court issued a written decision holding that the statute criminalised only theft of trade secrets produced for commerce or already in the marketplace, and that Goldman Sachs had no intention of selling or licensing its high-frequency trading platform. Indeed, the Court noted that Goldman Sachs went through great lengths to maintain the secrecy of the system since the profits generated depended on no one else having it, and thus, Aleynikov’s theft of the source code did not violate the EEA.

Criminal referrals vs traditional enforcement

In general, the DOJ’s recent focus on prosecuting IP crimes gives corporations another mechanism for protecting their proprietary information. Criminal prosecutions offer several clear benefits. As a general matter, an increase in IP prosecutions will deter the commission of these offences. Second, given the increasing globalisation of markets, the DOJ has significant resources and experience in pursuing targets and evidence in foreign countries, broad authority to conduct warrantless searches at the US border, and diplomatic means unavailable...
to private litigants. Third, a criminal prosecution may provide greater protection for a company’s remaining proprietary information than a protracted civil litigation because a criminal defendant has a limited right to discovery from the government and has no right to discovery from third parties. While there is a narrow right to subpoena third parties, it cannot be used as an end run around discovery and a court order is needed to require disclosure of information before the start of trial. Thus, corporations should consider criminal referrals in weighing potential options for responding to suspected thefts of trade secrets.

However, the Second Circuit’s narrow interpretation of the EEA is a setback for the DOJ and may influence the DOJ’s discretion in pursuing investigations based on a company’s report of a suspected trade secret misappropriation. While state prosecutors may nevertheless fill in the gaps, it is too early to tell whether these efforts will be successful. For example, Aleynikov is now facing criminal charges for violating two New York felony statutes – Unlawful Use of Secret Scientific Material and Unlawful Duplication of Computer Related Material – for the same conduct underlying his overturned federal conviction. The state action is pending in Manhattan’s criminal court.

While the full impact of the Second Circuit’s decision remains to be seen, it is likely to have a disproportionate effect on the financial sector and other industries that profit from the provision of services through the use of proprietary source code or other forms of intangible IP. Proprietary software integrated by companies into business methods to service their clients will likely fall outside the protections of the EEA. Specifically, companies that utilise source code for purposes other than licensing or sale in the marketplace, similar to Goldman Sachs’s high-frequency trading platform, will be vulnerable. Therefore, federal criminal referrals to protect against theft of employee trade secrets are likely to become less effective for proprietary trading firms and other technology-based businesses.

In many cases, traditional trade secret protection measures and civil enforcement tools remain the first, best and perhaps the only measures available to such companies seeking to protect their trade secrets. Civil litigation may be more advantageous for obtaining relief from harm caused by the misappropriation of proprietary information because a company can pursue the full range of traditional civil remedies including injunctions, compensatory and punitive damages, and reasonable attorney’s fees. While a victim may obtain restitution in a criminal case, it could take considerable time to be made whole.

Best practices in a post-Aleynikov world

As a preemptive measure, and in light of the Aleynikov decision with respect to technology-reliant businesses, companies with valuable trade secrets should re-examine their existing trade secrets protections. In many cases, formal trade secret audits should be conducted to identify the valuable information assets of the company and evaluate the strengths and weaknesses of its current protective measures. Further, in all cases, executives, human resources professionals and counsel should revisit and where necessary revamp their company’s procedures in the following areas:

- Restricted access to sensitive information;
- Management controls over use of external storage devices, copying of documents and data, email traffic, and tagging proprietary data;
- Use of restrictive covenants in employment agreements, employee handbooks and confidentiality policies, including: confidentiality or nondisclosure agreements; work-for-hire and assignment of inventions agreements; noncompete agreements; notice before termination (garden leave) provisions; reimbursement and forfeiture clauses; and liquidated damages and tolling provisions;
- Thorough exit procedures to ensure the security of proprietary data when employees depart, and use of models for tracing in the event of employee departures or security breaches; and
- Preparations to seek restraining orders and injunctions quickly in the event of misappropriations.

Despite the setback resulting from Aleynikov decision, the DOJ is likely to continue its aggressive enforcement of IP crimes in other sectors, particularly in the area of high-technology. The EEA remains an effective tool for combating the misappropriation of trade secret material for the vast majority of industries and marketed products. In addition, the Second Circuit ruling does not apply to the prosecution of foreign economic espionage under the EEA, even in the case of proprietary software. In charting the appropriate course of action once a company suspects it is a victim of trade secrets theft, corporate counsel will need to consider the legal and strategic complexities involved with making a criminal referral and/or proceeding with traditional civil enforcement.

More than ever, companies at risk of trade secrets theft should consult with experienced counsel to design the most effective strategy for protecting their valuable IP.

Footnotes

3. 18 USC § 1832
4. 18 USC § 1831
5. 18 USC §§ 1832(a), 1831(a)
6. 18 USC §§ 1832(a)(1)-(3), 1831(a)(1)-(3)
7. 18 USC § 1839(3)
8. 18 USC §§ 1832(a)(5), (b)
9. 18 USC §§ 1831(a)(4), 1831(b)
13. Id.
18. Criminal Complaint, People v. Aleynikov, No 60353/2012 (Sup Ct, NY County, 2012).

Jonathan B New is a partner in Baker Hostetler’s New York office, and formerly an Assistant US Attorney and DOJ Trial Attorney. Along with his white collar criminal and regulatory, internal corporate investigations and complex commercial litigation practice, he also counsels clients on IP and computer crimes.

Christy Nixon is a Baker Hostetler litigation associate, also in the New York office.