BERGER SINGERMAN
FLORIDA'S BUSINESS LAW FIRM

BIG AWARDS UNDERSCORE IMPORTANCE OF BOLSTERING YOUR COMPANY'S TRADE SECRETS PROTOCOLS

July 25, 2022

IPWatchdog

View Full Article

Corporate espionage is as old as the day is long. The modern digital world has made it easier than ever to gain access to sensitive “secret sauce”, such as software, customer and vendor lists, business methods, techniques, formulas and recipes. With a significant shift to a remote working environment and the relative ease of employee portability, protecting and defending confidential information and trade secrets must be at the top of the priority list for any organization.

In May 2022, in *Appian v. Pegasystems*, a jury awarded likely the largest sum in the history of Virginia state court proceedings, finding that Pegasystems was liable for $2 billion-plus in damages to Appian for planting a corporate spy at Appian for over 10 years. Through its plant (an operation Pegasystems internally referred to as “Project Crush”), Pegasystems was found to have misappropriated critical sensitive information about Appian’s cloud software, some of which was being developed under a government contract. The jury also found that Pegasystems’ employees, including its CEO, improperly used aliases to access trial versions of Appian’s software.

While the facts of the *Appian* case are not particularly unusual, the measure of damages is quite stunning. The $940 million dollar award in *Epic Systems Corp. v. Tata Consultancy Services Ltd.* is likely the only comparable case, and that award was eventually reduced to $280 million by the U.S. Court of Appeals for the Seventh Circuit. Although it seems possible, if not likely, that the Appian award will be reduced in appellate proceedings, the messaging is clear – courts and juries are now more than ever willing to hand out big penalties for trade secrets violations, particularly where there is evidence of intentional misconduct. The critical question, then, is how do organizations adequately protect themselves from corporate espionage and misappropriation in a rapidly developing remote and digital environment?

Employment Practices and Data Security

Organizations must pay significant attention to their hiring and retention practices and implement fail safes to avoid hiring potentially disloyal employees and detect unusual activity indicating that an active employee may be misappropriating sensitive information.

A thorough vetting process would include multiple interviews (including live, in-person interviews, even for remote positions), in-depth background searches as to financial, employment, and criminal histories and an investigation into the candidates’ internet and social media presence. Of course, these practices must be implemented in compliance with applicable state and federal employment practices, but most jurisdictions permit background checks and credit checks provided the employer obtains the candidate’s informed consent. The background check process can be greatly enhanced by interviewing colleagues and current employees in the relevant department about their knowledge and dealings with the candidate, professionally or otherwise.

Ultimately, it is now much easier to move between jobs and it does not take much for a disgruntled employee to decide to harm his employer by absconding with sensitive information shortly before leaving the company. Detecting disloyal current employees may be more daunting, but consideration should be given to regularly asking pointed questions to develop a greater understanding of an employee's psyche and attitude as their time with the company increases. Questionnaires in advance of quarterly or annual reviews might inquire about an employee's business activities or associations outside of the primary workplace (again, if compliant with applicable employment law).

Human resource managers and hiring partners must work cohesively with information technology and security departments to develop and implement safer employment practices. Proper data controls must be in place to identify and designate data with the proper level of secrecy, tier and compartmentalize access to that data, and track use and transfer of that data internally and externally. Most enterprise level file management software includes this functionality, and the cost of these resources has gone down significantly over the past several years. No organization is too small to implement data security protocols.

Incumbent with implementing these policies are proper employee onboarding documents such as non-disclosure agreements, non-competition agreements, and proprietary rights agreements. Many states recognize that the offer of continued employment is sufficient consideration to render enforceable such agreements with respect to current employees. Accordingly, care should be taken to regularly review these documents to assure they are up to date with current business realities and, when appropriate, issue updated acknowledgments to employees.

Intellectual Property Protection and Enforcement

Trade secrets are generally protected under state law (many states follow the ABA's Uniform Trade Secrets Act) and more recently under the Federal Defend Trade Secrets Act (18 U.S.C. § 1836). Critically, to be protected as a trade secret, the alleged protected material must be subject to reasonable measures to maintain secrecy. The standard of care for secrecy can vary greatly depending on the type of business involved. Software businesses are likely to be held to a higher standard than a local restaurant (even if the latter's barbeque sauce is one-of-a-kind). The burden lies solely with the organization to establish and implement secrecy protocols commensurate with the operations. Accordingly, the employment and IT practices discussed above are crucial to the organization's case in the event of litigation over data theft.

Other avenues of IP protection can be pursued alongside trade secret protection, with some important caveats. Written software code can be protected under United States Copyright law (17 U.S.C. § 101 et seq.). However, copyright owners should be careful in the registration process to designate as confidential all – or a portion – of the application for registration, which otherwise requires deposit material to be available to the public. If done correctly, an organization can pursue both trade secret and copyright infringement claims against the bad actors.

Patent protection is also extremely important but presents a significant tug-of-war with trade secret protection. Unless a non-publication request is filed, utility patent applications are published 18 months after the application filing date. Even if a non-publication request is filed (which requires the filer to forego foreign patent rights), the patent application becomes public if the application matures into an issued, enforceable patent. Thus, material in a patent application will generally be ineligible for trade secret protection. Given these constraints, an organization must carefully deliberate with patent counsel to determine what and how much of the "secret sauce" should be disclosed in a patent application before filing. Again, if done correctly, a party may be able to enforce both trade secret and patent infringement claims against the wrongdoer.

Related Practices

Corporate

Complex Commercial Litigation

Intellectual Property

Related Practice Teams

Business, Finance & Tax

Dispute Resolution

Related Team Member(s)

Geoffrey Lottenberg