BNA, INC.

ELECTRONIC COMMERCE & LAW

BNA Employee-Owned Since 1947

REPORT

Computer Crime

Brekka Case Shows Need for Comprehensive Strategy to Shield Data From Insider Misuse

The Ninth Circuit recently joined a trend disfavoring Computer Fraud and Abuse Act claims brought by companies against disloyal employees, employment and technology attorneys practicing within the circuit told BNA. *LVRC Holdings LLC v. Brekka*, No. 07-17116 (9th Cir. Sept. 15, 2009)(14 ECLR 1358, 9/23/09).

In *Brekka*, the court resolved disagreement among federal district courts within the circuit about how the CFAA's ''authorization'' standard applies to cases involving data theft by disloyal employees. The court explained that employers may be able to pursue claims under the CFAA (18 U.S.C. § 1030(g)), but only if employees violate clearly defined limits on access to company networks in the course of stealing proprietary information.

Employment and technology attorneys from the Ninth Circuit told BNA that the case set a high bar for corporate data protection policies to support CFAA claims, but highlighted the importance of clear policies on employees' use of corporate data no matter what causes of action are most appropriate in a given employee data misuse situation.

The bottom line, the attorneys explained, is that companies should draft confidentiality and technology policies with all potential causes of action in mind—trade secret, breach of contract, intellectual property infringement, and computer crime, among others—in order to most effectively protect their proprietary information from misuse by departing employees.

Trend Towards Narrowed Reading of CFAA. ''*Brekka* solidifies a trend of courts almost uniformly becoming less receptive to the CFAA as a cause of action in trade secret cases,'' Ilana Rubel, a technology attorney with Fenwick & West LLP in Los Angeles, told BNA.

''As a result, I would advise my clients to be more careful than ever in crafting confidentiality agreements that will protect them, as they are likely to have to rely on traditional state law causes of action in the case of absconding employees,'' Rubel said.

Companies have a number of legal options for pursuing employees who misuse sensitive corporate information, including lawsuits for breaches of nondisclosure agreements, misappropriation of trade secrets, conversion, and violations of intellectual property rights.

Brekka suggested that employers with carefully drafted policies might be able to pursue CFAA claims against disloyal employees, but companies should keep other causes of action in mind when drafting their confidentiality and employment policies because under *Brekka* the ability of an employer to succeed under the CFAA is by no means certain.

Because the standard for trade secret claims can be difficult to meet, companies should broadly define ''confidential information'' in confidentiality agreements, and preserve the right to seek injunctive relief against employees who violate the agreement, Rubel said. She also advised employers to consider seeking relief against any other actual or suspected recipient of the confidential information.

''Companies are not going to have a claim for 'unauthorized' use of their systems under the CFAA if they do not have a policy that explains acceptable uses of data and computer systems,'' Michael R. Overly, a technology attorney with Foley & Lardner LLP in Los Angeles, said. ''But they will still have other potential claims, including for a breach of an NDA or misappropriation of trade secrets.''

Employers should require employees to return all company data upon termination of employment, as well as delete it from any non-company devices and accounts to which it was transferred, Overly recommended. And if companies permit employees to transfer data to personal accounts or devices, they should have clear standards for what they can do with it, he said.

 ISSN 1098-5190

''I don't know how significant this ruling is going to be because employers have other remedies beyond the CFAA, but the decision does indicate that their computer access policies must be clear,'' Jim Goodman, an employment partner with EpsteinBeckerGreen in Los Angeles, said.

''Companies should make sure that their policies or agreements with their employees spell out that e-mailing documents to personal accounts is prohibited, or require that electronic data transferred from the company to personal accounts be returned or destroyed,'' Goodman advised.

The message from *Brekka*, according to Carolyn Sieve, attorney with Seyfarth Shaw LLP in Los Angeles, is that employers should not rely solely on a potential CFAA claim to protect their proprietary information. ''The *Brekka* decision places more responsibility on the employer's shoulders to provide notice to employees as to what is 'authorized' access.''

Employers should determine what information they want to protect, implement security protocols to safeguard that information, and combine those efforts with systematic employee education regarding confidentiality and data use policies, Sieve recommended.

***Brekka* Resolves Circuit 'Authorization' Uncertainty.** The Ninth Circuit's *Brekka* ruling resolved some unanswered questions within the circuit about when a disloyal employee accesses company data ''without authorization.''

The CFAA, at 18 U.S.C. § 1030(g), provides a civil cause of action against parties that access computers ''without authorization'' or who ''exceed authorized access,'' and commit one of several enumerated offenses that causes damage or loss.

Prior to *Brekka*, several federal district courts within the Ninth Circuit ruled that employees acted ''without authorization,'' and thus violated the CFAA, once they breached duties of loyalty to their employers and continued accessing employers' computer networks. But at least one rejected that line of reasoning in a 2008 opinion that has been widely cited outside the circuit.

Brekka rejected that agency-based approach to the issue, which the Seventh Circuit explained in *International Airport Centers v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (11 ECLR 303, 3/15/06). There the court said that an employee can lose otherwise authorized access to a computer by breaching a duty of loyalty to the company, or otherwise consciously acting against the company's interest.

Several federal district courts within the Ninth Circuit have followed *Citrin*. For example, in *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.*, 119 F.Supp.2d 1121 (W.D. Wash. 2000)(5 ECLR 1127, 11/15/00), the court said that an employee may access a company computer ''without authorization'' if he does so for the purpose of sending proprietary information to a competitor.

Similarly, in *ViChip Corp. v. Tsu-Chang Lee*, 438 F.Supp.2d 1087 (N.D. Cal. 2006), the court followed *Citrin*, granting summary judgment to a company under the CFAA against a former CEO who deleted computer files.

But the U.S. District Court for the District of Arizona flatly rejected *Citrin* in *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962 (D. Ariz. 2008)(13 ECLR 350, 3/12/08). The CFAA prohibits unauthorized access, not data misuse, *Gast* said.

''*Brekka* cements the Ninth Circuit on the anti-*Citrin* approach to the 'authorization' issue,'' Rubel said.

In *Brekka*, the court said that an employer's ability to pursue a former employee for alleged data misuse under the CFAA will depend on how its policies restrict employees' access to data on its computer systems. The court held that a company could not pursue CFAA claims against a former employee who forwarded corporate documents from his work computer to a personal account.

The employee was not working under any sort of an employment contract, nor was there any policy against e-mailing proprietary information. The court concluded that '' 'authorization' depends on actions taken by the employer.''

If the company could have proven that the employee remotely accessed corporate servers after his termination, the court said, then there would have been a viable CFAA claim because that use was never authorized from the start. But the company's allegations on this point were unpersuasive, and the court refused to assign liability ''based on mere speculation.''

BY AMY E. BIVINS

Full text at http://pub.bna.com/eclr/07cv17116_091509.pdf

  ECLR ISSN 1098-5190