Computer Fraud & Abuse Act: Court Rejects Argument That Employer's Corporate Policies Can Make Employee Access "Unauthorized" Under the CFAA

Insights
11.23.10

No sooner than we posted last week's blog regarding the dismissal of the United States' Computer Fraud and Abuse Act ("CFAA") claims against Sergey Aleynikov in the Goldman Sachs' high-frequency trading code criminal prosecution, a California federal district court issued a similar noteworthy opinion dismissing CFAA claims against an employee who was accused by his former employer of using the employer's computer systems to misappropriate trade secrets and confidential information. Accenture, LLP v. Sidhu, No. C10-2977-TEH (N.D. Cal., Nov. 9, 2010). A pdf copy of the Court's opinion is available below.

As readers of this blog know well by now, the CFAA provides a federal, private right of action against any person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value... ." 18 U.S.C. § 1030(a)(4).

There is a division within the federal judiciary over whether the CFAA applies to a faithless employee's misappropriation of his or her employer's confidential information or trade secrets by means of the employer's computer, to which the employee had authorized access as a result of his or her employment. On this legal issue, there is a continuum of interpretations of the CFAA within the federal judiciary. Some district and appellate courts hold that the CFAA gives employers a federal cause of action against their disloyal departing employees, in what has been perceived as a pro-employer interpretation. On the other end of this continuum are what would appear to be employee-centric opinions holding that the CFAA does not create such a right in employers. (Some bloggers, such as our respected colleague, Marc Dobin of Jupiter, Florida openly advocate for the employee centric view.)

Along the continuum of decisions, the Sidhu opinion is more employee-centric, and several aspects of the court's analysis support this perception. Sidhu was an employee of Accenture. Accenture alleges that during an extended medical leave, Sidhu started working for HCL, Accenture's direct competitor. However, Accenture contends that for the duration of Sidhu's medical leave, Accenture made available to Sidhu its secure online network containing confidential and proprietary information. According to Accenture, Sidhu downloaded more than 900 documents from Accenture's proprietary computer KX system while on medical leave and, notably, after he began working for HCL. Accenture had two company-wide corporate policies that were relevant to its CFAA claims:

HOL. Accenture had two company-wide corporate policies that were relevant to its CFAA claims: first, a policy that prohibited employees from transmitting work documents to their personal computers and, second, a policy that prohibited dual-employment. As is often true in these types of cases, the ultimate facts are likely to be hotly contested.

After Accenture filed suit, Sidhu filed a motion to dismiss, and the court dismissed Accenture's CFAA claims. The court's analysis was grounded in LVRC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), where an appellate court held that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." Brekka, 581 F.3d at 1133. Under the CFAA, the phrase "exceeds authorized access … means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This statutory definition "implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer," the Brekka court observed. Brekka, 581 F.3d at 1135. As the court reasoned, an individual only "exceeds authorized access" if he has permission to access a portion of the computer system but uses that access to "obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter."

In holding that Sidhu was given access to Accenture's computers by Accenture, the court rejected Accenture's arguments that it limited Sidhu's access through its corporate policies. First, Accenture argued that it implemented policies that prohibited its employees from transferring documents from work computers to personal computers. Sidhu, at * 9-10. "[A]ccess is not established by employers' policies, but by the extent the employer makes the computer system available to the employee," the court concluded. Id. at *10.

Also rejected by the court was a variant of the agency theory of the CFAA's access provision. Under this theory, an employee is an agent of his or her employer. Such agents are authorized to access their employers' computer systems as long as the agents are loyal. However, as soon as the employee undertakes a disloyal act – such as misappropriating trade secrets or confidential information in order to compete against the employer – the agency is terminated. Under this theory, the disloyal employee would be unauthorizedly accessing his or her employer's computer systems.

The variant of the agency theory argued by Accenture emphasized its policy that prohibited dual employment. During Sidhu's medical leave, Accenture argued, Sidhu lied to Accenture's human resources and began working for Accenture's competitor. Given these allegations, and under the agency theory, Sidhu's access to Accenture's computer system was unauthorized, according to Accenture. This argument was rejected by the court as an attempt to "incorporat[e] corporate policy into the substance of the CFAA," the court held. Id. at *11. "Whether Sidhu was deceptive, and whether he would have been fired pursuant to Accenture's Dual Employment Policy had Accenture learned of his deception, are irrelevant.' Id. at * 12.

These explicit rejections of an employer's attempt to restrict access to its computers through corporate policies crystallizes the importance of taking concrete steps in order to limit employee

access to trade secrets and confidential information residing on an employer's computer systems. Under the reasoning employed in Sidhu, simply saying that an employee may not access information under certain circumstances may not be enough.

Brent Cossrow is a member of Fisher Phillips Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below.

Accenture v. Sidhu.pdf (81.92 kb)

Related People

Brent A. Cossrow
Regional Managing Partner
610.230.2135
Email