Crowell

Client Alert

California Court Recognizes Narrowly Drawn CFAA Claim Against Traffickers of Access Credentials

January 30, 2013

In a blow to victims of data theft, the Ninth Circuit in *United States v. Nosal* held less than a year ago that the Computer Fraud and Abuse Act (CFAA) was not an available remedy where the alleged thief had authorized access to the computer system from which data was stolen. The Northern District Court of California's recent decision in *Oracle America, Inc. v. Service Key, LLC* (No. 12-00790) may well breathe new life in the CFAA by recognizing claims against hackers who not only steal but traffic access credentials.

Oracle alleged that DLT Federal Business Systems Corporation obtained log-in credentials to its technical support websites through a program for authorized resellers of Oracle's enterprise hardware and software systems. Oracle also alleged that DLT fraudulently used its credentials to obtain Oracle's proprietary software products and distributed those products, as well as the log-in credentials, to provide support services to third parties. Oracle alleged that these actions violated several subsections of the CFAA.

The court recognized that, under *Nosal*, accessing a company's computers is not actionable under the CFAA so long as the user has authorization to access the computers. Thus, the court held that, because DLT has legitimate access credentials, the use of those credentials to obtain and distribute Oracle's software products to unauthorized third parties was beyond the scope of the CFAA.

But the court determined that Oracle could proceed with a CFAA claim under a subsection that prohibits the fraudulent trafficking of "any password or similar information through which a computer may be accessed without authorization" where such trafficking affects interstate or foreign commerce. 18 U.S.C. § 1030(a)(6). The court held that *Nosal*'s interpretation of "exceeds authorized access" was "not germane" to Oracle's trafficking claim and could stand if properly pled.

Directly contrary to the approach taken by many district courts across the country, the court also held that the heightened pleading requirements of Rule 9(b) of the Federal Rules of Civil Procedure apply to CFAA claims. According to the court, Oracle's allegations that DLT "falsely represented to its customers and potential customers that it could still obtain—from [DLT]—software patches and updates for their Oracle computer products" and "engaged in the fraudulently trafficking of passwords to facilitate third-party access" to Oracle's websites were "grounded in fraud" and thus must be pled with particularity.

Victims of data theft should take note of this court's decision. While the decision underscores the limited reach of the CFAA for actions pending in courts within the Ninth Circuit, it nonetheless recognizes a potentially new avenue for relief where hackers access without authorization computer systems for the purpose of providing unauthorized access to others. This decision also raises the bar to plead certain CFAA claims with the specificity normally reserved for typical common law fraud claims.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Ellen Moran Dwyer
Partner – Washington, D.C.
Phone: +1.202.624.2574
Email: edwyer@crowell.com