Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY
AND E-DISCOVERY AND INFORMATION
MANAGEMENT

DECEMBER 2015

Second Circuit Draws Line Between Employees and Hackers Under Computer Fraud and Abuse Act

Employers in New York face a heightened hurdle to holding employees legally accountable for theft and other misuse of company data after the Second Circuit's recent decision in *United States v. Valle*. The Court has held that it is not enough to show that an employee with authorization and login credentials to the company network misused their access in violation of the company computer use policy; companies must now show that the employee did not have authorization and bypassed a technological barrier to access the information. Valle provides further incentive for employers to revisit their technical security measures to ensure their data is safe not only from outside attack, but also from untrustworthy employees.

The Computer Fraud and Abuse Act of 1986 (CFAA) imposes criminal and civil liability on one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer." The Act defines a protected computer as "a computer affected by or involved in interstate commerce." Because all computers with Internet access are affected by interstate commerce, an employer's computer will typically be "protected" for purposes of the CFAA. Accordingly, any employer who suffers damage or loss by reason of an employee's violation of the CFAA may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.

Employers often assert claims under the CFAA against disloyal employees who take company data – such as customer lists – when they depart to join a competitor. To prove that an employee is civilly liable under the CFAA, an employer must show that the employee "exceeded authorized access." A split has developed in the courts as to whether an employee with authorization and login credentials to the company system "exceeds authorized access" by misusing their access in violation of the employer's computer use policy. The First, Fifth, Seventh, and Eleventh Circuits have held that an individual may "exceed authorized access" simply by violating the company policy. On December 3, 2015, however, the Second Circuit issued its decision in Valle and joined the Fourth and Ninth Circuits in the minority of the circuit split, holding that mere violation of a company policy does not amount to a violation of the CFAA.

In *Valle*, New York City police officer Gilberto Valle was criminally charged with violating the CFAA after he used his access to NYPD computer programs for non-law enforcement purposes. According to NYPD policy, officers are only permitted to access these databases in in the course of an officer's official duties. Instead, Valle ran searches to obtain information about individuals who were the subject of his personal fantasies. Despite the disturbing nature of the facts, the *Valle* Court held that the defendant did not "exceed authorized access" within the meaning of the CFAA because the NYPD had given him permission to access the database. This holding effectively limits violations of the CFAA to instances when an individual circumvents some technological barrier to access information that he or she does not have authorization to access for any purpose. The Court reasoned that if it were to adopt a broader construction of the CFAA language, even the most trivial violation of a company policy, such as checking one's Facebook page, would be a federal crime.

In light of the Second Circuit's ruling, employers in New York, Connecticut and Vermont should take technical security measures to restrict computer access to active employees only, and to restrict particular sets of data to those employees who properly require access. Access should be limited by written policies in addition to technological barriers such as encryption and firewalls. Doing so not only preserves the employer's ability to bring a civil action under the CFAA, but also fortifies the employer's cybersecurity practice in general. For more information, please contact Clifford G. Tsan (315.218.8252; ctsan@bsk.com) or Allison Zullo Gottlieb (646.253.2313; agottlieb@bsk.com).

Christopher J. Dioguardi, a 2015 law graduate who is awaiting admission to the New York bar, co-wrote this Information Memo.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond