THE NATIONAL LAW JOURNAL
SEPTEMBER 26, 2015
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

Time Is Precious with Computer-Hacking Claims

A recent ruling shows that plaintiffs must act fast when using a federal criminal statute for a civil suit.

BY NICK AKERMAN


WILLIE B. THOMAS

The U.S. Court of Appeals for the Second Circuit in August addressed the proper application of the statute of limitations to a civil action—in the context of allegations of malicious statements made on the Internet over a broken romance and sexual misconduct—brought under the federal computer crime statute, the Computer Fraud and Abuse Act (CFAA). The case was *Sewell v. Bernardin*.

The CFAA, primarily a criminal statute, permits those who have suffered damages or loss due to a violation of the CFAA to bring a civil action to obtain compensatory damages and injunctive relief. However, for the cause of action to be valid, it must be brought within two years "of the date of the act complained or of the date of the discovery of the damage."

Sewell underscores the need for immediate action upon discovering a data breach to investigate and identify the perpetrator of the computer crime.

Chantay Sewell sued her former boyfriend Phil Bernardin, who had gained access to her private AOL email and Facebook accounts through passwords he had allegedly gathered when visiting Sewell. She was the only authorized user of both accounts and never shared her passwords with Bernardin. According to her complaint, Sewell discovered that she could no longer log into her AOL account because someone had changed her email password. Shortly thereafter, malicious statements directed at Sewell linking her with "certain sexually transmitted diseases and sexual activities" were emailed from within her email account to her family and friends, whose contact information was contained in Sewell's email account.

Some five months later, Sewell also discovered that her Facebook account had been compromised, and she was unable to log into her Facebook account. Shortly thereafter, someone

posing as Sewell posted on Facebook similar malicious statements about Sewell's "sex life." After the Facebook discovery, Sewell filed a lawsuit alleging, among other things, two violations of the CFAA, one for the intrusion into her AOL account, and the other for the intrusion into her Facebook account.

In her complaint, Sewell alleged that Bernardin had obtained her passwords "without her permission." A critical element of a CFAA violation is that the defendant accessed the accounts "without authorization." Verizon records showed that Bernardin had used his computer to access Sewell's AOL and Facebook accounts and changed Sewell's passwords.

The district court dismissed the CFAA claims on the ground that "Sewell was 'aware that the integrity of her computer had been compromised' " when she first discovered the change to her AOL password and that discovery started the running of the two-year statute. The Second Circuit affirmed the district court's dismissal of the CFAA claim based on the AOL intrusion for failing to comply with the statute of limitations. However, it reversed the district court on the later Facebook CFAA intrusion, holding that the filing occurred within the CFAA's two-year statute of limitations.

The Second Circuit faulted the district court for assuming that "because one password for one Internet account was compromised," all of Sewell's Internet accounts had been compromised.

The appeals court took judicial notice "of the fact that it is not uncommon for one person to hold several or many Internet accounts, possibly with several or many different user names and passwords, less than all of which may be compromised at any one time." The appeals court also pointed out that the CFAA claim on the AOL account was not premised on Sewell's own physical computer but "on impairment to the integrity of a computer owned and operated by AOL."

'TROUBLING CONSEQUENCES'

The Second Circuit acknowledged that the statute of limitations "may have troubling consequences in some situations" because "the investigation necessary to uncover the hacker's identity may be substantial." One option the court recognized was for a plaintiff to file a John Doe lawsuit to uncover the hacker's identity. However, the court emphasized that the hacker's identity still must be discovered within two years because "Rule 15(c) does not allow an amended complaint adding new defendants to relate back if the newly-added defendants were not named originally because the plaintiff did not know their identities."

Two district courts outside the Second Circuit recently granted expedited discovery requests to Internet Service Providers in John Doe CFAA actions to learn the identities of the hackers. Those are *Jockey Club Information Systems v. John Doe*, in the Eastern District of Kentucky, and *Uber Technologies v. John Doe*, in the Northern District of California. In *Jockey Club* the plaintiff alleged that the hackers "accessed and stole proprietary data" from its website using "sixty different internet protocol ... addresses to make over one million requests per day." In *Uber* the plaintiff was seeking to identify the hackers who accessed its website to steal "confidential details on the drivers" who use its "smartphone application that connects drivers and riders in cities all over the world."

In both cases, the plaintiffs met the uniform good-cause standard for permitting expedited discovery, including showing: first, the John Doe defendant is a real person who can be sued; second, unsuccessful efforts to locate and identify the defendant; third, the action can withstand a motion to dismiss; fourth, discovery is likely to identify the defendants; and fifth, the likelihood that ISPs will not preserve the information sought.

The obvious takeaway from *Sewell* is that potential CFAA plaintiffs must act immediately to identify the perpetrator once a computer hack is discovered.

NICK AKERMAN *is a partner in the New York office of Dorsey & Whitney, where he focuses on the Computer Fraud and Abuse Act, the Racketeer Influenced and Corrupt Organizations Act, federal trade secrets law and post-employment restrictive covenants.*