Win for Apple on Its iPhone Operating System: Computer Fraud and Abuse Act Claim Dismissed

A critical element in proving either a civil or criminal violation of the Computer Fraud and Abuse Act ("CFAA"), the federal computer crime statute, is that the defendant act with criminal intent as opposed to mistake or negligence. In discussing the breadth of computers covered by the CFAA the Eight Circuit emphasized the importance of this critical element of intent: "[w]hat protects people who accidentally erase songs on an iPod, trip over (and thus disable) a wireless base station, or rear-end a car and set off a computerized airbag, is not judicial creativity but the requirements of the statute itself: the damage must be intentional." *U.S. v. Mitra*, 405 F.3d 492, 495-96 (8th Cir. 2005). Indeed, the CFAA expressly provides that a defendant who is charged with violating the CFAA for damaging a computer must be shown to have "intentionally caus[ed] damage without authorization." 18 U.S.C. § 1030 (a) (5) (A) (i).

This past summer, as part of a class action suit against Apple, Inc. ("Apple") and AT&T Mobility, LLC alleging various causes of action including the Sherman Antitrust Act, a California federal court granted summary judgment to Apple dismissing the CFAA claim because of a lack of proof that Apple had intended to damage consumers' iPhones with its 1.1.1 Operating System Software. *In re Apple & ATTM Antitrust Litigation*, 2010 WL 3521965 *5-7 (N.D. Ca. July 8, 2010).

The CFAA claim was premised on the plaintiffs' claim that "they lost third party applications [on their iPhones] when the 1.1.1 Software bricked [made inoperable] their iPhones and they were unable to use their iPhones for a period of days after their iPhones were bricked." *Id*. at *5. These third party applications apparently cost the plaintiffs "between $10 and $70." *Id*. at *6. The court found that the plaintiffs had not established standing because they had "not produced sufficient evidence of injury resulting from the 1.1.1 Software" since Apple had promptly provided them with "a free replacement iPhone," and there was not "sufficient evidence of harm based on loss of third party software applications." *Id.* at *7.

Nonetheless, the court held that even if the plaintiffs had established such evidence of harm, they had "not produced sufficient evidence to show that the Defendant Apple acted with an intent to damage Plaintiffs' iPhones with the 1.1.1 Software." *Id.* at 7. In particular, the court found that "Plaintiffs have not produced documents or testimony showing that Defendant Apple designed the 1.1.1 Software to "brick" iPhones containing third party applications," and therefore the "Plaintiffs have failed to introduce specific evidence to create [a] triable issue that in offering the 1.1.1 Software, Apple acted with intentional conduct to cause Plaintiffs harm." *Id.*

The court also found it significant that the Plaintiffs failed to produce 'any evidence that they were required to download and install the 1.1.1 Software," but "[i]nstead, they each

voluntarily installed it." *Id*. Thus, the court concluded that this "[v]oluntary installation runs counter . . . to CFAA's requirement that the act was 'without authorization." *Id.*

This case is significant because it underscores the legal requirement that a CFAA claim can only be successful if the plaintiff is able to prove criminal intent. Non-criminal practitioners who traditionally file civil lawsuits can easily lose sight of the fact that the CFAA is essentially a criminal statute, and that even though a civil case need only be proven by a preponderance of the evidence as opposed to the beyond a reasonably doubt criminal standard, the CFAA still requires proof of the traditional criminal element of intent.