CLIENT ALERT

Allegation of Data Breach Alone Insufficient to Sustain Claims Based on Inadequate Cybersecurity

Mar.15.2013

On March 6, 2013, the United States District Court for the Northern District of California held that a putative class of LinkedIn premium users lacked standing to pursue state law unfair competition, breach of contract, and negligence claims resulting from a hacking incident. The court dismissed the complaint, concluding that the plaintiffs failed to establish any legally cognizable injury and any causation between the alleged incident and any alleged economic harm.

LinkedIn, the online community for professional networking, offers both free and premium paid accounts to consumers. The Privacy Policy applicable to both types of accounts provides that user information will be protected with "industry standard protocols and technology," but notes that it provides no guarantee that LinkedIn's security will be able to prevent all security breaches. On June 6, 2012, hackers infiltrated LinkedIn's computer systems and posted 6.5 million user passwords and email addresses. LinkedIn subsequently updated its password encryption method to prevent future breaches.

A putative class of premium LinkedIn users filed an amended complaint alleging unfair competition, breach of contract, and negligence claims. LinkedIn filed a motion to dismiss for lack of standing, which the court granted.

The plaintiffs claimed that they suffered "economic harm" because they were denied the full benefit of their bargain for the paid premium memberships. Specifically, the plaintiffs alleged that they would not have purchased the premium product absent the security guarantees, and that the 2012 hacking incident shows they did not receive the promised security. The court rejected the plaintiffs' "economic harm" argument for several reasons.

First, the plaintiffs failed to show that they paid consideration for LinkedIn's promise to safeguard their information because the same security policies applied equally to the free and paid accounts. Second, unlike situations involving food-labeling misrepresentations, the plaintiffs did not allege that they actually read the alleged misrepresentation—the Privacy Policy—and thus failed to show a causal relationship between the misrepresentation and any injury. Third, the plaintiffs failed to show that the alleged breach of contract (*i.e.*, failing to provide the security promised in the Privacy Policy) caused the economic loss (*i.e.*, not receiving the full benefit of the bargain). Instead, the court concluded that the injury could only have occurred before the hacking incident at the time the parties entered into the contract. This particular aspect of the opinion addressing the timing of the alleged injury is likely to be the subject of debate. It was not, however, the sole basis for rejecting the plaintiffs' economic harm allegations. Indeed, the court also made clear that where plaintiffs allege harm from a defective product, plaintiffs must show "something more" than the economic harm of "overpaying for the defective product." Here, the plaintiffs alleged only that LinkedIn provided defective security, not that LinkedIn provided a product different than what the plaintiffs purchased. Consequently, the court concluded that the plaintiffs would need to allege "something more" resulted from the defective security, such as identity theft, which they did not do.

In addition to rejecting the plaintiffs' "economic harm" arguments, the court also held that the increased risk of future harm did not establish an injury sufficient to confer standing. The court concluded that the plaintiffs failed to state a legally cognizable injury by merely alleging that their passwords were publicly posted as opposed to alleging identity theft.

Based on the pleadings before it, this court concluded that the mere allegation of a security breach does not automatically confer Article III standing or provide the basis for cognizable state common law claims. Rather, the failure here to allege an injury beyond "overpaying" for a service, *e.g.*, identity theft, required dismissal of these claims. The court also rejected the plaintiffs' claimed injury stemming from an increased risk of future identity theft, deeming it speculative and thus insufficient to sustain the claims. This decision bolsters the "lack of standing" defense to claims premised on security breaches brought in federal court. The case is *In re LinkedIn User Privacy Litigation*, 2013 WL 844291 (N.D. Cal. Mar. 6, 2013).

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

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com