Recent California Decision Demonstrates Challenges Faced By Plaintiffs In Data Breach Litigation

On July 11, 2013, the U.S. District Court for the Central District of California granted a motion for judgment on the pleadings with respect to the majority of claims brought against Blizzard Entertainment, Inc. ("Blizzard") in the wake of a data breach suffered by Blizzard in 2012. U.S. District Judge Beverly Reid O'Connell dismissed the plaintiffs' class action claims for unjust enrichment, negligence, breach of contract and bailment, permitting only the Delaware consumer protection counts to proceed. The *Blizzard* decision highlights the difficulties faced by plaintiffs asserting class claims in the wake of a data breach.

Plaintiffs alleged that in 2008, in an effort to increase account security, Blizzard introduced the "Authenticator," which creates a random code that account holders must enter when logging into Blizzard games. On August 4, 2012, Blizzard became aware that hackers had gained access to account holders' information, and the breach was announced five days later. The hackers gained access to account holders' email addresses, answers to personal security questions, and cryptographically scrambled versions of account passwords. While one of the two named plaintiffs utilized the Authenticator, the other named plaintiff had not acquired an Authenticator; each named plaintiff purported to represent a class of similarly situated individuals.

To begin with, while the district court refused to grant Blizzard's motion for judgment on the plaintiffs' claims for violations of the Delaware Consumer Fraud Act ("CFA"), its ruling on this point was a narrow one. The court first determined that plaintiffs had not alleged sufficient facts demonstrating that Blizzard failed to take steps to ensure the security of account holders' information under the heightened pleading standards applicable to fraud-based claims. However, Judge O'Connell then considered plaintiffs' contentions that Blizzard should have disclosed that to have security in their account safety, account holders had to purchase an "Authenticator." The court found that Blizzard did not sufficiently respond to that issue with respect to plaintiffs' claims under the Delaware CFA, and thus denied Blizzard's motion for judgment as to the Delaware CFA counts in that respect.

However, Blizzard won judgment on all of plaintiffs' common-law claims. The court granted Blizzard's motion for judgment with respect to plaintiffs' unjust enrichment claim after determining that plaintiffs failed to challenge Blizzard's conduct on a basis not governed entirely by the parties' contractual agreements – namely, the Terms of Use and Privacy Policies. The court thereby concluded that an unjust enrichment claim was barred under Delaware law.

In granting Blizzard judgment with respect to plaintiffs' negligence and breach of contract claims, Judge O'Connell held that plaintiffs failed to show any cognizable harm from the August 2012 breach. Citing data breach precedent applying Delaware law, the court explained that an increased risk of future identity theft is insufficient to support a negligence claim. Furthermore, the court explained that any damages flowing from diminution of the video games' value would be barred under a negligence theory by the economic loss doctrine, which prohibits recovery in tort for purely economic injuries, because plaintiffs failed to identify any duty that Blizzard breached other than the duties imposed by its contracts with customers. Moreover, plaintiffs' breach of contract claim failed because plaintiffs alleged only speculative damages. The court also granted Blizzard's motion with respect to bailment, stating that "[no] court has held that personal information is a chattel that can be bailed." With the exception of bailment, plaintiffs were given leave to amend their common-law claims.

The *Blizzard* opinion highlights the difficulties faced by plaintiffs asserting claims on behalf of a putative class in the wake of a data breach. First, *Blizzard* follows a long line of federal and state court cases dismissing negligence claims based on data breaches for lack of cognizable injury. Plaintiffs have been particularly unsuccessful at demonstrating injury where, as in *Blizzard*, they could not allege any identity theft. Furthermore, as courts in data breach matters have dismissed claims other than negligence due to lack of cognizable injury, including negligent misrepresentation and consumer protection claims, the impact of *Blizzard*'s injury analysis will likely reach beyond the negligence context.

In addition, *Blizzard* demonstrates the challenges that data breach plaintiffs face in navigating among the various legal doctrines that apply to common-law claims. As in *Blizzard*, where plaintiffs and defendants possess a contractual relationship, courts often reject plaintiffs' efforts to press non-contractual claims such as for negligence and unjust enrichment, on the ground that the contract should provide the sole common-law remedy for breach of contractual duties. However, where no direct relationship exists with defendants, plaintiffs are particularly vulnerable to the argument that defendants owe them no common-law duty in tort, and thus their tort claims fail as a matter of law. Earlier this year, for instance, a magistrate judge recommended dismissal of negligence claims that consumers had brought against payment processor Global Payments, Inc. over a data breach because the consumers possessed a direct relationship only with the merchants that accepted their credit cards, not with the defendant Global Payments. Absent a direct relationship, the judge reasoned, Global Payments owed the consumers no duty of care.

For more information regarding the *Blizzard* decision and its potential impact, please contact a member of our leading privacy and data security team, including **Doug Meal**, **Mark Szpak**, **Jim DeGraw**, and **David McIntosh**.