Federal Court Dismisses Action Brought by Data Breach Plaintiffs for Failure to Demonstrate Injury Under *Clapper*

On September 3, 2013, the U.S. District Court for the Northern District of Illinois dismissed a class action complaint arising from a credit card "skimming" attack suffered by Barnes & Noble in 2012. U.S. District Judge John W. Darrah held that plaintiffs failed to demonstrate standing under Article III of the U.S. Constitution, and therefore could not proceed with their complaint for breach of contract, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), invasion of privacy, violation of the California Security Breach Notification Act, and violation of the California Unfair Competition Act. The *Barnes & Noble Pin Pad* decision highlights the ongoing challenges faced by plaintiffs in data breach litigation to articulate injury both for purposes of Article III standing and in order to state a claim for relief.

Barnes & Noble uses PIN pads to process its customers' credit and debit card payments at retail stores. On October 24, 2012, Barnes & Noble announced it had experienced a security breach, whereby so-called "skimmers" potentially stole customer information transmitted through PIN pad devices at sixty-three Barnes & Noble retail locations in nine states, including Illinois and California. "Skimming" is a form of electronic hacking that enables the unauthorized collection of credit and debit card data. Approximately six weeks after learning of the attack (according to the complaint), Barnes & Noble publicly announced the breach and published a notice on its website instructing its customers to take precautions against identity theft and fraud.

Four customers who had made purchases at Barnes & Noble stores located in Illinois and California brought suit in the wake of the announcement. The plaintiffs asserted a wide variety of damages due to the security breach, including: an increased risk of identity theft, untimely and inadequate notification of the security breach, improper disclosure of plaintiffs' personal identification information ("PII"), invasion of privacy, expenses incurred and time lost to mitigate the increased risk of identity theft or fraud, deprivation of the value of their PII, anxiety and emotional distress, and overpayment for Barnes & Noble products due to security measures the company failed to provide. One plaintiff also alleged she suffered a fraudulent charge on her credit card after the security breach.

Relying on the Supreme Court's decision earlier this year in *Clapper v. Amnesty International*, Judge Darrah granted Barnes & Noble's motion to dismiss for lack of standing. At the outset, the court explained that to establish standing under *Clapper*, a plaintiff must demonstrate that they have suffered an "injury in fact" that is "certainly impending," and that allegations of possible future injury fail to meet the test outlined by the Supreme Court. Judge Darrah then reviewed the injuries asserted by plaintiffs, holding each of them insufficient under *Clapper*.

The court began its analysis by explaining that a mere increased risk of identity theft or fraud fails to establish standing under *Clapper* because speculation of future harm does not constitute actual injury. While plaintiffs argued that *Clapper* only required a "substantial risk" of injury, Judge Darrah held that plaintiffs' allegations also fell short of this test. The court similarly disposed of plaintiffs' statutory claims, explaining that even if plaintiffs could show that Barnes & Noble violated the statute in question, any such violation would be insufficient to establish standing without actual injury.

With respect to plaintiffs' supposed loss of privacy and improper disclosure of their PII, the court held that the plaintiffs had not sufficiently alleged that their PII was disclosed in the security breach. Citing *Clapper*, the court further held that expenses incurred to mitigate an increased risk of identity theft or fraud cannot

establish standing in the context of non-imminent harm. Similarly, Judge Darrah explained that emotional distress in the wake of a security breach is insufficient to establish standing, particularly absent any imminent threat to the plaintiffs' PII.

The court dismissed the plaintiffs' argument that they had been deprived of the value of their PII, noting that the plaintiffs did not allege they had the ability to sell their information. The judge similarly was not persuaded that the plaintiffs suffered injury by overpaying for Barnes & Noble products in light of security measures the company failed to provide, noting that plaintiffs did not allege that Barnes & Noble charged higher prices for transactions using credit cards. Finally, the court held that the sole plaintiff who alleged a fraudulent charge failed to plead actual injury because she did not allege that she was not reimbursed for the charge.

The *Barnes & Noble Pin Pad* opinion highlights the significant hurdle now imposed by *Clapper* for data breach plaintiffs. While numerous courts have dismissed data breach actions for failure to state a claim due to lack of injury, *Barnes & Noble Pin Pad* suggests that data breach cases post-*Clapper* increasingly will be decided on standing grounds, and that speculation of future harm will not suffice. To the extent such claims continue to survive Article III scrutiny, Judge Darrah's injury analysis also undermines the likelihood such allegations will be held sufficient to state a claim for relief. Furthermore, the opinion suggests that even where a data breach plaintiff alleges actual misuse of information, the allegations will not constitute cognizable injury where the plaintiff fails to allege that he or she was not reimbursed for the charges. Finally, as Article III applies to all data breach matters brought in federal court, the impact of Judge Darrah's injury analysis reaches well beyond the causes of action asserted in *Barnes & Noble Pin Pad*, and will extend to other claims, such as negligence and negligent misrepresentation, frequently asserted in the data breach context.

For more information regarding the *Barnes & Noble Pin Pad* 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.