Online Retailer Zappos.com Reaches Settlement with Nine Attorneys General Over Data Security Breach

Last week, the online shoe and clothing retailer Zappos.com, Inc., reached a settlement with nine state Attorneys General over a 2012 data security breach that allegedly exposed the personal information of more than 24 million customers. The settlement requires Zappos to pay $106,000 and undergo a security audit. The states' action against Zappos reflects the latest example of how states are handling privacy and data security breaches, which all companies that collect or use consumer information can face.

The Attorneys General launched an investigation of Zappos in January 2012, within days of the company's announcement of an unauthorized intrusion into its internal computer network and systems via one of the company's servers in Kentucky. The breach reportedly exposed information about millions of customers, including names, email addresses, billing and shipping addresses, phone numbers, the last four digits of payment card numbers, and encrypted passwords. There apparently was no evidence that full credit or debit card numbers or other payment data was compromised in the breach. Zappos notified the affected customers of the breach, advising them to reset their passwords on Zappos.com and other websites where they use similar credentials.

The settlement agreement requires Zappos to make a monetary payment of $106,000, to be divided among Arizona, Connecticut, Florida, Kentucky, Maryland, Massachusetts, North Carolina, Ohio, and Pennsylvania. Zappos also agreed to hire an independent third party to conduct an information security audit of its security regarding personal information, provide the Attorneys General with a copy of the audit, and address any identified deficiencies. In addition, Zappos agreed to maintain, update as needed, and comply with security policies to protect personal information, including those policies concerning vulnerability assessments and patch management. Further, the company must provide the Attorneys General with copies of its security policies and reports reflecting its compliance with industry-wide data security standards, and institute at least annual employee training programs regarding its security policies. These non-monetary provisions of the settlement run for a duration of two years.

The settlement with Zappos provides an important illustration of the manner in which state Attorneys General address such cases. States have initiated inquiries against businesses of all sizes that have suffered data security breaches or have been accused of privacy violations, contending that the businesses should have done more to protect consumers' information. They have done so even where, as in the Zappos case, the companies were clearly victimized by outside criminal attacks and only limited types of information were exposed. And they have done so even when the Federal Trade Commission, which aggressively asserts authority over privacy matters under the Federal Trade Commission Act and other federal statutes, has opted not to proceed. These state actions can involve coordinated efforts by Attorneys General from many (and sometimes dozens) of states, and this collaboration is expected to continue in the coming months and years as data security breaches continue to be reported in ever-increasing numbers. All companies that collect or use consumer information should proactively review their policies and practices to minimize these enforcement risks, and if a regulatory investigation begins, they should retain counsel competent in navigating the complexities of multistate actions from the start.

For more information regarding the settlement between Zappos and the nine Attorneys General or to discuss data security practices generally, please feel free to contact a member of Ropes & Gray's leading Privacy & Data Security team or your regular Ropes & Gray contact.

James S. DeGraw
Douglas H. Meal
Mark P. Szpak