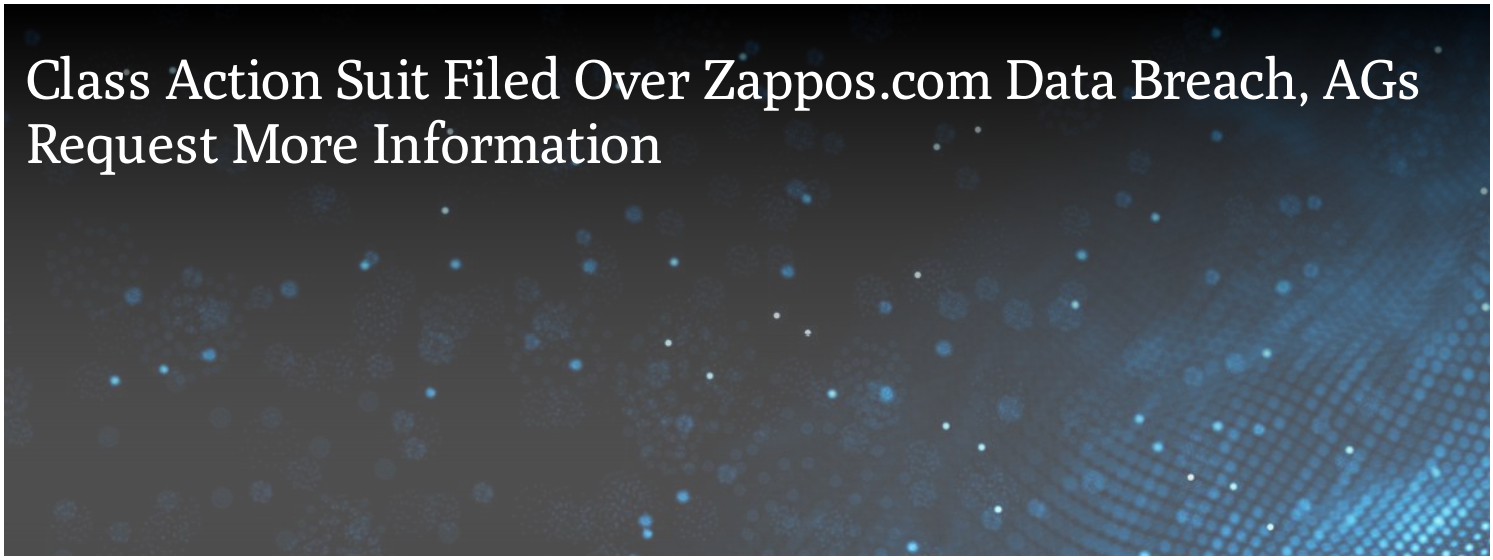
WINSTON & STRAWN LLP

BLOG

Class Action Suit Filed Over Zappos.com Data Breach, AGs Request More Information



FEBRUARY 1, 2012

A complaint was filed on January 16, 2012 in Kentucky against Amazon.com on behalf of a putative class of some 24,000,000 customers of Zappos.com, which is owned by Amazon.com. The suit alleges that Amazon violated the Fair Credit Reporting Act ("FCRA"), when it allowed a hacker to access part of its internal network and systems, enabling the hacker to gain access to customer personal information such as names and addresses, email addresses, phone numbers, encrypted passwords, and the last four digits of credit card numbers (the hacker did not access the database that stores credit card and other payment data). The complaint was filed less than 24 hours after Zappos sent out a notice to its customers. The complaint alleged that Amazon failed to adopt and maintain adequate procedures to protect such information and limit its dissemination only for the permissible purposes set forth in the FCRA, which also constituted common law invasion of privacy and negligence by not properly securing the servers that stored defendants' personal information. Although the breach did not expose customer's social security numbers, nor did it expose complete credit card information, the complaint nevertheless alleged that class members were harmed, because they would have to take the time to change their passwords on the Zappos.com website as well as their email accounts and any other Web sites where they used the same password. The complaint further alleges that class members are now more susceptible to identity theft, resulting in anxiety, emotional distress, and loss of privacy. In addition to the lawsuit, the Attorneys General of nine states, including Connecticut Kentucky, Florida, Massachusetts, North Carolina, New York and Pennsylvania sent a letter to Amazon seeking additional information about the incident.

Tip: This lawsuit serves as a reminder that class action lawyers and Attorneys General may watch breach notifications closely. Companies can act proactively by putting in place the strong security programs, as are appropriate for the types of information that they maintain. Being prepared to respond in the event of a data breach, not only in the consumer-notification phase, but also in the event of any subsequent inquiries, is also prudent.

1 Min Read

Related Topics

Financial Privacy | Data Breach | Consumer Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2025 Winston & Strawn LLP.