



importance of maintaining cybersecurity measures – assessing the ashley madison data breach settlement

Aaron Wais
MSK Client Alert

December 16, 2016

practice areas

immigration

Daily headlines of data breaches, resulting class actions, governmental investigations and enforcement actions, and the settlements of those actions serve as constant reminders of the need to implement and maintain reasonable cybersecurity measures. Yet another example can be found in the recent announcement by the Federal Trade Commission, which states that the operators of Ashley Madison have agreed to settle the charges brought against them by the FTC and over a dozen state attorneys generals arising out of the July 2015 data breach of Ashley Madison's network. Analyzing the settlement also provides additional guidance on what regulators mean when they refer to reasonable safeguards.

In its complaint, the FTC alleged that Ashley Madison's parent company, Ruby Corp. (f/k/a Avid Life Media, Inc.), and a pair of related entities failed to adequately protect their approximately 36 million users' accounts and profile information. (The FTC also alleged various misrepresentations that are not relevant here.) According to the FTC complaint, the defendants collected a broad range of personal information from its customers, including full names, addresses, dates of birth, payment card numbers, sexual preferences and desired encounters. The defendants also collected and maintained their customers' communications with each other, such as messages and chats.

[View Full Alert](#)