# *Client Alert*: Cheaters Never Win: Ashley Madison Settles FTC and State Data Security Charges for $1.65 Million

**Related Attorneys**

Scott M. Guttman

**Related Services**

Data Strategy, Privacy and Security

Litigation

**CLIENT ALERT** | 12.14.2016

Today, the FTC and 13 states announced a settlement with notorious website Ashley Madison related to its July 2015 data breach that exposed the personal information of more than 36 million users.

According to the FTC, until August 2014, the site lured customers by using fake profiles of fake women, which were designed to convert the customers into paid membership. Only paid membership allowed use of all the site features, such as sending messages, chatting online in real time, and sending virtual gifts. The website promised users their personal information such as date of birth, relationship status and sexual preferences was private and securely protected, through statements such as the website was "100% secure," "risk free," and "completely anonymous." The homepage also prominently displayed a "Trusted Security Award" icon indicating the website was an "SSL Secure Site", as well as a "100% Discreet Service" image.

Despite these promises, the FTC and state attorneys general alleged that in fact the website's security was insufficient, because:

- no written information security policy was in place;
- no reasonable access controls were in place;
- inadequate security training of employees;
- the defendants had no knowledge of whether third-party service providers were using reasonable security measures; and
- no measures to monitor the effectiveness of system security were in place.

According to the FTC, hackers were able to access the companies' networks several times between November 2014 and June 2015, but due to the lax data-security practices, the intrusions were not discovered. This led to the breach announced on July 12, 2015, and in August of 2015, the hackers published sensitive profile, account security, and billing information for more than 36 million AshleyMadison.com users. Notably, according to the FTC, the published information included information on users who had paid $19 for a "Full

Delete" service to purportedly delete their data from the site, but in fact, had been retained by Ashely Madison. From December 2012 through December 2015, US consumers had paid a total of $2,388,566 for this Full Delete Option.

The settlement requires Ashely Madison to implement a comprehensive data security program, including third party assessments of its program every two years. The settlement also prohibits the company from misrepresenting its privacy and security measures, including the extent to which users can control or delete their information, the number of actual users, and prohibits the use of fake profiles.

Approximately half of the settlement will be paid to the FTC, and the remaining funds will be split among the 13 states and the District of Columbia that participated in the settlement. For some states, such as Arkansas, Oregon and Vermont, this settlement comes on the heels of their recent $1M settlement with Adobe in connection with Adobe's 2013 data incident involving the personal information of 534,000 individuals. 15 states participated in this settlement.

So, what's the lesson from this settlement? According to the FTC, "[B]usinesses must keep their promises. And if you collect sensitive personal information, you must protect it." Additionally, regulators like the FTC and state attorneys general expect businesses to have reasonable data security measures in place, and will enforce their laws against businesses who fail to meet that standard. For questions on data security programs, breach response, breach preparedness or planning, please contact Heather Enlow-Novitsky, Scott Guttman or your Vorys attorney.