# One Less (Regulator) Affair for AshleyMadison.com: Site Operators Agree to Settle U.S. Charges Stemming from 2015 Breach

Dana B. Rosenfeld, Alysa Z. Hutnik

December 23, 2016

Remember the 2015 AshleyMadison.com data breach, where hackers gained access to the personal information of about 36 million users from over 46 countries, and threatened and carried through on their promise to release the information to the public? This highly publicized incident has resulted in a $1.6 million settlement between operators of the dating website and the FTC, 13 states, and the District of Columbia, resolving allegations concerning inadequate security and deceptive practices connected to the website. The FTC also received investigative assistance from the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner, both of which had concluded a joint investigation of the dating website in August.

The FTC's complaint charges AshleyMadison.com with:

- **Creating Fake Profiles to Encourage Consumers to Upgrade Services**. AshleyMadison.com staff created 24,414 female "engager profiles," or fake profiles, through which staff would communicate with AshleyMadison.com users. According to the FTC, AshleyMadison.com staff used these engager profiles to entice users to upgrade to a full membership.

- **Failing to Remove Consumer Profiles Despite Representations to Consumers That Profiles Would be Deleted**. AshleyMadison.com advertised a service option to users that enabled them to delete their "digital trail." The company charged consumers for this service, but did not disclose until after the purchase was consummated that some information would be retained for legal and financial reasons. Moreover, the company in some instances altogether failed to remove or delete consumer profiles from internal systems.

- **Prominently Displaying/Advertising that the Site was Secure When Evidence and Practice Suggested the Contrary**. AshleyMadison.com advertised their website as "100% secure", "risk-free", and "completely anonymous" and prominently displayed data security trustmarks (seals or icons designed to give consumers confidence in a company's data security practices). One such trustmark was a "Trusted Security Award," which the FTC says the company never received. AshleyMadison.com also advertised a privacy policy that touted "industry standard" security safeguards the company employed to protect against loss or unauthorized access. The FTC alleged this was deceptive given the inadequate security practices that contributed to the 2015 data breach.

- **Failing to Provide Reasonable Security**. AshleyMadison.com did not take reasonable steps to prevent unauthorized access to their systems. According to the FTC, the company did not:
    - Maintain a written information security policy
    - Implement reasonable access controls
    - Provide adequate training for personnel with data security responsibilities
    - Have adequate measures in place to vet third-party service provider security measures
    - Use readily available security measures to monitor systems for data security events and verify the overall effectiveness of their security systems

As companies target consumers across borders and expand their global consumer reach, they should pay close attention to this global settlement and consider implementing proactive compliance measures to properly safeguard consumer data and avoid practices that can cause irreparable harm to consumer confidence and company reputation.