THE
NATIONAL LAW REVIEW

Website Hacks Result in FTC Actions for Lax Security

Friday, May 17, 2019

After hacks of two websites, i-Dressup.com and ClixSense.com, resulted in the compromise of personal information for millions of users – including, in the case of i-Dressup, hundreds of thousands of children under 13 – the Federal Trade Commission (FTC) issued complaints against the websites and their operators for lax security and other privacy violations. Notably, in addition to requiring beefed-up security and third-party monitoring programs in the settlement agreements, all five FTC Commissioners took the additional step of holding senior management personally responsible for data security in the future. In a separate statement, the Commissioners wrote:

KELLER AND HECKMAN LLP

Article By Tracy P. Marshall
Sheila A. MillarKeller and Heckman LLP
Consumer Protection Connection

Communications, Media & Internet
Administrative & Regulatory
All Federal

The orders obtained in these matters contain strong injunctive provisions, including new requirements that go beyond requirements from previous data security orders. For example, the orders include requirements that a senior officer provide annual certifications of compliance to the Commission, and explicit provisions prohibiting the defendants from making misrepresentations to the third parties conducting assessments of their data security programs.

i-Dressup allows users to design their own virtual outfits and try on different looks. The FTC complaint against i-Dressup claims the website and its operators violated the Children's Online Privacy Protection Act (COPPA) on several grounds: (1) failing to provide reasonable security, which resulted in a hacker stealing the personal information of 2.1 million users, including 245,000 children; (2) failing to obtain parental consent before collecting personal information from children under 13; and 3) continuing to collect children's personal information even when parents refused to give consent.

ClixSense pays users to view ads and take online surveys. Users who registered with the site were required to provide personal information, including names, addresses, passwords, user names, and (in some cases) Social Security numbers. Despite assurances that "ClixSense utilizes the latest security and encryption techniques to ensure the security of your account information," the FTC complaint charges that the company failed to protect the website from commonly known or reasonably foreseeable vulnerabilities and attacks from third parties and failed to perform vulnerability and penetration testing. This lax security led to a data breach in September 2017 in which hackers downloaded the personal information of 6.6 million users worldwide. The hackers then published and offered for sale the personal information of 2.7 million users, including names and addresses, user names, passwords, email addresses, and Social Security numbers.

Under iDressup's agreement with the FTC, the company will pay $35,000 in civil penalties and is required to implement a comprehensive data security program that is subject to independent third-party monitoring. Under its settlement with the FTC, ClixSense's owner is barred from misrepresenting the company's security and data collection practices, and like iDressup, must also implement a comprehensive information security program that is subject to independent monitoring.

Imposing personal responsibility on senior management demonstrates the seriousness with which the FTC views data privacy and data security obligations. The Commissioners' statement ends with a presage for the future: "the announcements today reflect the beginning of our thinking, but we anticipate further refinements, and these orders may not reflect the approach that we intend to use in every data security enforcement action going forward." Online businesses, take note.

Source URL: https://www.natlawreview.com/article/website-hacks-result-ftc-actions-lax-security