HINSHAW

Alerts

FTC Lessons Learned: Encrypt Consumer Data When Your Privacy Policy Says You Encrypt Consumer Data

June 16, 2021
Hinshaw Privacy & Cyber Bytes

Once again, we see that inaccurate information in a privacy policy can land an organization in hot water. On June 7, 2021, the Federal Trade Commission (FTC) announced a proposed settlement with MoviePass pertaining to its "one movie per day" subscription plan. While the FTC's primary complaint involved deceptive advertising of its subscription plan, the proposed settlement also addressed a data breach that occurred after MoviePass left an unencrypted database exposed—which lead to unauthorized access to consumer personal information—as well as inaccuracies in MoviePass's representations concerning its cyber and privacy practices. It also mandates key steps MoviePass must take to implement an effective Information Security Program.

The FTC Complaint

As outlined in its complaint, the FTC took issue with a number of MoviePass's business practices. First, the FTC alleged MoviePass deceptively advertised its "unlimited" movie viewing subscription package because it devised and implemented a "password disruption" and "ticket verification" program that limited the frequency with which subscribers could view movies.

With respect to data privacy and cybersecurity, the FTC alleged MoviePass failed to take reasonable measures to secure consumer data. The business collected personal information, including first name, last name, postal address, email address, birth date, gender, credit card number, CVV, expiration date, billing address, card type, geolocation information, user reviews, and movies attended. The FTC alleged that MoviePass's privacy policy represented that it "takes information security very seriously" and "uses reasonable administrative technical, physical, and managerial measures to protect [consumers'] personal details from unauthorized access." MoviePass also represented that it stored consumer email addresses and payment information in "an encrypted form."

On August 20, 2019, however, a security researcher was reported to have breached an exposed database containing consumer personal information. MoviePass confirmed the data breach, which exposed a server containing unencrypted personal information. Financial and other personal information of over 28,000 consumers was affected.

Service Areas

Privacy, Security & Artificial Intelligence

The FTC alleged the breach was made possible because MoviePass:

- Stored personal information in clear text;
- Failed to conduct periodic risk assessments or perform vulnerability and penetration testing;
- Disabled firewalls;
- Failed to provide adequate security training to its employees; and
- Failed to implement safeguards to detect anomalous activity and/or cybersecurity events.

The Proposed Settlement

The proposed settlement prohibits MoviePass from misrepresenting certain terms of its subscription plan. MoviePass is also barred from *misrepresenting* that it will take reasonable administrative technical, physical, or managerial measures to protect consumers' personal Information from unauthorized access.

MoviePass will need to implement an Information Security Program that includes the following, among other components:

- Documenting the content, implementation, and maintenance of its Information Security Program;
- Providing the written program, evaluations, and updates to its Board of Directors every 12 months and within 30 days of a data breach;
- Designating a qualified employee or employees to coordinate, oversee, and be responsible for the Information Security Program;
- Training all of its employees at least once every 12 months on how to safeguard personal information;
- Technical measures to monitor all of its networks and all systems and assets within those networks to identify data security events;
- Testing and monitoring the effectiveness of its safeguards; and
- Selecting and retaining service providers capable of safeguarding the personal information they access.

MoviePass will also need to obtain an initial, and then biannual, third-party assessment of its Information Security Program and cooperate with a third-party information security assessor.

The Takeaways

Privacy policy 101 is to *Say what you do and Do what you say*. So when your privacy policy says that you encrypt personal information—encrypt it. And when your privacy policy says that you use "reasonable administrative, technical, and physical" safeguards, know what that means and confirm that you are implementing those safeguards. Enterprises should regularly review their privacy policy to ensure its accuracy and that the enterprise's business practices are aligned with all compliance requirements.

The proposed settlement also provides the foundation for an effective Information Security Program that businesses collecting, storing, using, and sharing personal information should have in place.

The list above is the tip of the iceberg. See the proposed settlement for more details.