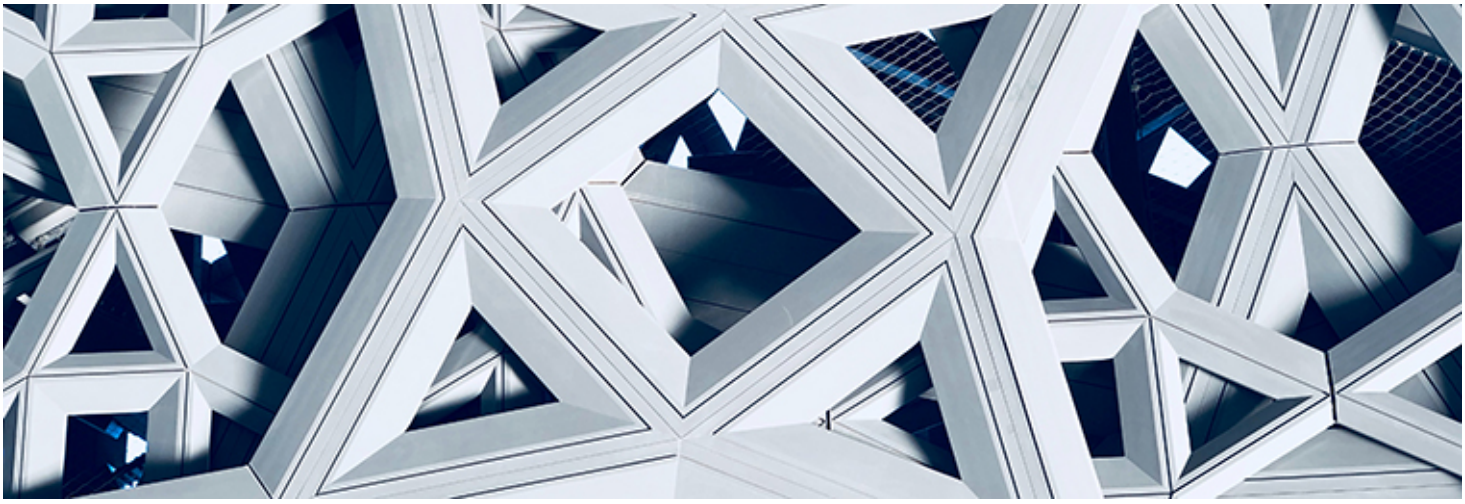

CafePress to pay $500,000 for FTC violations

Cybersecurity Law Alert

22 March 2022
By: Andrew Serwin | Emily Maus | Deborah R. Meshulam | Leila Javanshir

On March 15, 2022, the FTC announced an administrative complaint and proposed consent agreement against the former and current owners of CafePress over allegations that it failed to secure consumers' sensitive personal data collected through its website and covered up a major breach. The FTC's proposed order requires the company to not only strengthen its information security program, but also requires the former owner of the company to pay $500,000 to be used for consumer redress.

The FTC's action is just the latest in an ongoing series of government actions (discussed here and here) seeking to address cybersecurity risks. It highlights government expectations that companies maintain robust cybersecurity programs and provide appropriate disclosures and reports regarding security breaches.

The FTC's action

CafePress hosts an online platform where consumers nationwide and internationally can purchase customized merchandise. The FTC alleged that the failure by CafePress to implement reasonable security measures led to multiple breaches of its network.

These failures allegedly included:

- Storing personal information in readable text
- Failing to implement reasonable measures to protect passwords
- Failing to implement a process to receive and address vulnerability reports from third parties
- Failing to implement patch policies and procedures
- Failing to establish or enforce rules to make user credentials sufficiently complex
- Storing personal information indefinitely without a business need to do so
- Failing to implement reasonable procedures to prevent, detect or investigate an intrusion and
- Failing to respond reasonably to security incidents.

In February 2019, CafePress allegedly experienced a data breach affecting customer information associated with a significant number of user accounts, which exposed millions of emails and passwords, addresses, security questions and answers as well as a smaller number of Social Security numbers, partial payment card numbers and expiration dates. This information was later discovered for sale on the dark web.

After being notified of the intrusion into its network and confirming its customer information had been obtained by an unauthorized person, the company patched the vulnerability, but allegedly failed to properly investigate the breach.

The FTC alleged that affected customers weren't notified of the incident until September 2019, after the breach was reported by the press. The FTC alleged that CafePress was aware of security issues prior to the 2019 breach, calling out that it had experienced hacked accounts and malware infected servers and employee computers in 2018. According to the FTC, the 2018 incidents were never adequately investigated or resolved.

Pursuant to the order, the company must implement and maintain a comprehensive information security program that meets the minimum requirements set forth by the FTC within the order. Some of the notable requirements include replacing its authentication via security questions and answers with multifactor authentication and encrypting Social Security numbers on the company's network.

The company's lack of information security measures was not the only failure called out in the complaint. The FTC also alleged that the company's privacy practices were misleading. Specifically, the FTC alleged that CafePress collected email addresses from customers and used those email addresses for marketing purposes despite representations of a more limited use. The company also failed to honor its commitments related to deleting consumer information in accordance with applicable law.

Key takeaways

Certain aspects of the agency's action deserve particular attention:

- Although not explicit, the order appears to imply that failure to timely notify consumers of a breach, or concealing a breach, constitutes an unfair and deceptive practice under Section 5 of the FTC Act.
- While the proposed settlement calls for the former owner to pay $500,000 "in redress to victims of the data breaches," the agreement fails to specify the authority on which the FTC relies to issue such redress. The concept of a redress fund in this context is fairly novel for the FTC and might be a result of the recent Supreme Court ruling limiting the FTC's ability to obtain certain forms of equitable relief .
- As part of the comprehensive security program, CafePress must replace its authentication via security questions and answers with multi-factor authentication. *This is the first time the FTC has explicitly flagged security questions and demanded multi-factor authentication.* It even goes so far as to recommend cryptographic software or authenticator applications as secure authentication protocol, discouraging multi-factor authentication through SMS.
- The comprehensive security program also requires "[p]olicies and procedures to minimize data collection, storage, and retention." This is unusual for the FTC to include in a data security focused order and appears related to concerns in the complaint that sensitive data, such as social security numbers, were retained for longer than necessary. It may signal new attention from the FTC on data minimization and overcollection of unnecessary consumer data.

While there are many notable aspects to the FTC settlement, it is also notable that this settlement occurred as many other

agencies, including the SEC continue to sharpen their focus on the disclosure of cyber issues, as well as the level of cyber controls that companies have.

See the FTC's press release here.

Learn more about the implications of this case by contacting any of the authors.

AUTHORS

Andrew Serwin
Partner
San Diego (Golden Triangle) | T: +1 858 677 1400
andrew.serwin@dlapiper.com

Emily Maus
Associate
Washington, DC | T: +1 202 799 4000
emily.maus@dlapiper.com

Deborah R. Meshulam
Partner
Washington, DC | T: +1 202 799 4000
deborah.meshulam@dlapiper.com

Leila Javanshir
Associate
Seattle | T: +1 206 839 4800
Leila.Javanshir@dlapiper.com