Published on *The National Law Review* https://natlawreview.com

FTC Settles with Company Over Alleged Deceptive Security Practices

Article By:

Kari M. Rollins

Julia K. Kadish

The FTC recently settled with smart lock maker Tapplock, Inc., a Canadian company, over allegations that it deceived consumers with false claims about its product's security practices. These allegations arose based on vulnerabilities that a security researcher demonstrated – not in the aftermath of a data security breach where these complaints often originate.

In its complaint, the FTC cited claims Tapplock made in its product advertisements, including that the product was "secure," with an "unbreakable" design. The FTC also noted that Tapplock's privacy policy stated that the company deployed "reasonable precautions and follow[s] industry best practices to make sure [personal information] is not inappropriately lost, misused, accessed, disclosed, altered or destroyed."

However, security researchers pointed out a number of alleged physical and electronic vulnerabilities. For example, by unscrewing the back panel, a researcher was able to unlock the product within a few seconds. The lack of encryption on the Bluetooth communication between the lock and the app also allowed a researcher to discover and replicate the private keys necessary to lock and unlock the product. There were also issues with how user access was revoked, essentially allowing even revoked users an ability to later authenticate access to another user's lock.

The FTC alleged that these product vulnerabilities, combined with a lack of certain compliance measures such as: vulnerability testing, written data security policies and procedures, and privacy and security guidance and training for employees designing the software meant that the company was contrary to its security claims of "reasonable precautions" and "industry best practices."

As part of the settlement, Tapplock will be required to implement a comprehensive information security program, train employees at least once a year on safeguarding personal information, use certain data access controls, and conduct vendor management. Tapplock must also obtain independent third-party assessments of its program every two years and submit that assessment to the FTC for approval.

Putting it Into Practice: This settlement highlights that even in the absence of a data breach, the

FTC may look to researchers and other evidence finding security vulnerabilities in products and services that may be contrary to claims made about privacy and security. This settlement also highlights the importance and value the FTC (like other regulators) places on having written information security policies and procedures, regular data security training for employees, and periodic vulnerability tests and security audits; companies will be served by acting proactively to implement or establish such compliance measures. For organizations based outside the US, this settlement also serves as a reminder of certain factors the FTC may look to when evaluating whether a non-US company is targeting US consumers. Namely, the FTC cited the fact that the product was advertised in U.S. dollars, and fulfilled by a service provider in the US and shipped to a US-based warehouse (and the website refenced this fact).

National Law Review, Volume X, Number 112