

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman  
Noah Joshua Phillips  
Rohit Chopra  
Rebecca Kelly Slaughter  
Christine S. Wilson

In the Matter of  
  
TAPPLOCK , INC., a corporation.

DOCKET NO. C-4718

COMPLAINT

The Federal Trade Commission ("Commission") having reason to believe that Tapplock, Inc. ("Respondent" or "Tapplock") has

2. The acts or practices of Respondent alleged in this complaint have been in interstate commerce, as "commerce" defined in Section 4 of the Federal Trade Commission Act, and constitute "deceptive acts or practices involving foreign commerce" within the meaning of Section 5 of the FTC Act.

'S BUSINESS PRACTICES

3. Respondent is an Internet of Things ("IoT") company that, among other things, sells Internet-connected, fingerprint-enabled padlocks ("smart locks") to U.S. consumers. Respondent's smart locks interact with a companion mobile application ("app") that U.S. users are able to download onto their mobile devices. This app logs usernames, email addresses, profile photos, location history, and precise geolocation of a user's smart lock, and it allows users to lock and unlock their smart locks when they are within Bluetooth range.
4. Respondent designs the smart locks it sells to U.S. consumers, is responsible for remediating security vulnerabilities and other flaws associated with those locks, and directly or through its distributors markets and advertises its locks to consumers.



10. Respondent makes additional claims about its information security practices in its privacy policy, accessible online to its U.S. customers, stating in part:

To protect your personal information, we take reasonable precautions and

15. Contrary to the statements described in Paragraph 8-11, Respondent did not take reasonable measures to secure its locks, or take reasonable precautions or follow industry best practices for protecting consumers' personal information. In fact, Respondent did not have a security program prior to the discovery of the vulnerabilities described in Paragraph 13 and 14. For example, Respondent:
- a. failed to identify reasonably foreseeable risks to the security of its smart locks or the security of customers' personal accounts, such as through vulnerability or penetration testing, and assess the sufficiency of any safeguards in place to control those risks;
  - b. failed to employ sufficient measures to detect and prevent users from bypassing the authentication procedures in Respondent's API to gain access to other users' accounts;
  - c. failed to adopt and implement written data security standards, policies, procedures, or practices; and
  - d. failed to implement adequate privacy and security guidance or training.

information provided by consumers. Therefore, the representation set forth in Paragraph 19 is false or misleading.

Violation of Section 5

21. The acts and practices of Respondent as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this eighteenth day of May 2020, has issued this complaint against Respondent.

By the Commission.

April J. Tabor  
Acting Secretary

SEAL: