**192 3011**

**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*** | **DOCKET NO.** |
| **TAPPLOCK, INC., a corporation.** | |

# COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Tapplock, Inc. ("Respondent" or "Tapplock") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Tapplock, Inc. is a Canadian corporation with its principal office or place of business at 121 Richmond Street West, Toronto, Ontario M5H 2K1, Canada.

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

## RESPONDENT'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, e-mail addresses, profile photos, location history, and the 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 U.S. consumers.

5. Respondent advertises to U.S. consumers through its website, www.tapplock.com, and has previously advertised through the online crowd funding website Indiegogo.com. These websites advertised Respondent's smart locks in U.S. dollars.

6. Further, Respondent contracted with a U.S.-based third-party service provider to fulfill orders and ship its products to U.S. consumers.

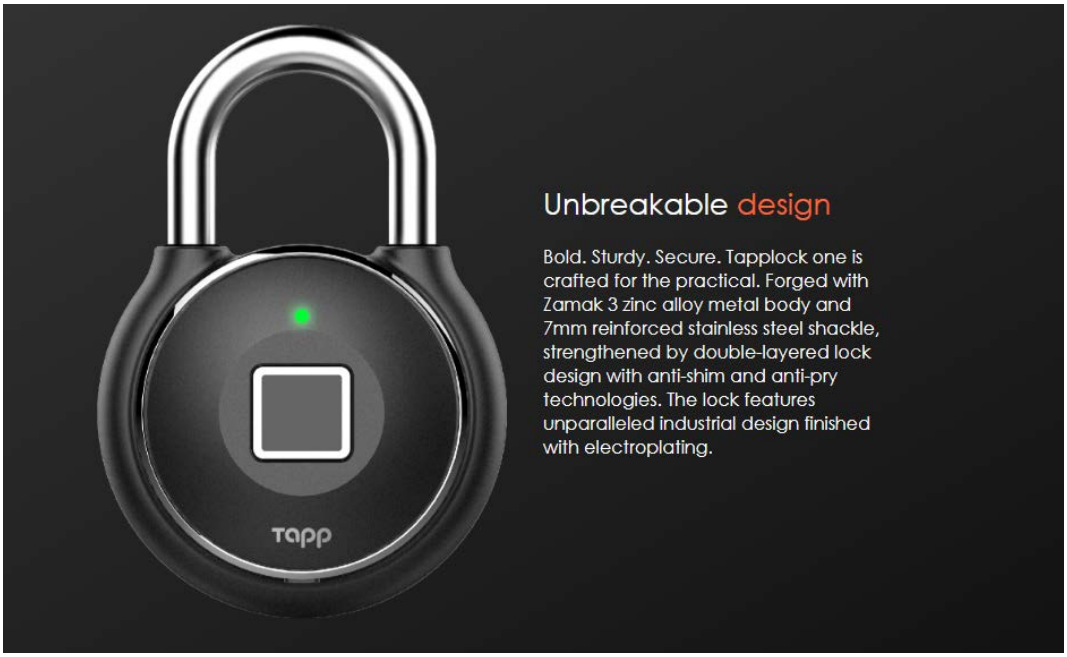
7. Respondent shipped its devices to its service provider's U.S.-based warehouse in order to fulfill orders to U.S. customers. Respondent also referenced the U.S.-based warehouse in public statements to customers (e.g., "Our warehouse is in New Jersey").

## RESPONDENT'S DECEPTIVE SECURITY PRACTICES

8. Respondent advertised its smart locks to consumers as "Bold. Sturdy. Secure."

9. Respondent's advertisements touted that its "secure" smart locks were also:

- "strengthened with double-layered lock design;"
- designed with "anti-shim and anti-pry technologies" (Shimming refers to inserting a foreign object into the latch, and prying refers to using a lever to force open a padlock); and
- designed to be "unbreakable," as follows,



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 follow industry best practices to make sure it is not inappropriately lost, misused, accessed, disclosed, altered or destroyed.

11. Respondent also claims that users can share access to their locks with an unlimited number of other people, and that users can subsequently limit or revoke such shared access.

12. Despite these claims, Respondent's smart locks were not secure. In June 2018, three separate security researchers identified critical physical and electronic vulnerabilities with Respondent's smart locks.

13. With respect to physical security, one security researcher demonstrated that he could unlock some of Respondent's smart locks within a matter of seconds, simply by unscrewing the back panel.

14. Researchers also discovered reasonably foreseeable electronic security vulnerabilities that could have been avoided if Respondent had implemented simple, low-cost steps. For example:

    a. One vulnerability in Respondent's API allowed researchers to bypass the account authentication process in order to gain full access to the accounts of all Tapplock users and their personal information, including usernames, e-mail addresses, profile photos, location history, and precise geolocation of smart locks. A researcher who logged in with a valid user credential could then access another user's account without being re-directed back to the login page, thereby allowing the researcher to circumvent Respondent's authentication procedures altogether.

    b. A second vulnerability allowed researchers to lock and unlock any nearby Tapplock smart lock. Because Respondent failed to encrypt the Bluetooth communication between the lock and the app, researchers were able to easily discover and replicate how Respondent generated the private keys necessary to lock and unlock user's smart locks.

    c. A third vulnerability prevented users from effectively revoking access to their smart lock once they had provided other users access to that lock. This vulnerability allowed the researchers to "sniff" data packets for the information necessary to authenticate their access to the lock. With that information, researchers were able to continue accessing the lock even after their access had been revoked.

15. Contrary to the statements described in Paragraphs 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 for its employees responsible for designing, testing, overseeing, and approving software specifications and requirements.

16. As a result of these failures, consumers' personal information was exposed, as described in Paragraph 14, and consumers' personal property was put at risk.

## VIOLATIONS OF THE FTC ACT

### Deceptive Representation Regarding Security (Count I)

17. Through the means described in Paragraphs 8-9, Respondent has represented, directly or indirectly, expressly or by implication, that its smart locks were secure.

18. In truth and in fact, as described in Paragraphs 12-16, Respondent's smart locks were not secure. Therefore, the representation set forth in Paragraph 17 is false or misleading.

### Deceptive Representation Regarding Protection of Personal Information (Count II)

19. Through the means described in Paragraph 10, Respondent has represented, directly or indirectly, expressly or by implication, that it took reasonable precautions and followed industry best practices to protect the personal information provided by consumers.

20. In truth and in fact, as described in Paragraphs 14-16, Respondent failed to take reasonable precautions and follow industry best practices to protect the personal

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 ___ day of ____, 2019, has issued this complaint against Respondent.

By the Commission.

[April J. Tabor]
[Acting Secretary]

SEAL: