



[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 192 3011]

Tapplock, Inc.; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement; Request for Comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order – embodied in the consent agreement – that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY**

INFORMATION section below. Write “Tapplock, Inc.; File No. 192 3011” on your comment, and file your comment online at <https://www.regulations.gov> by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Jared Ho (202-326-3463), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Website (for March 30, 2020), at this web address: <https://www.ftc.gov/news-events/commission-actions>.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Write “Tapplock, Inc.; File No. 192 3011” on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the <https://www.regulations.gov> website.

Due to the public health emergency in response to the COVID-19 outbreak and the agency’s heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the <https://www.regulations.gov> website.

If you prefer to file your comment on paper, write “Tapplock, Inc.; File No. 192 3011” on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at <https://www.regulations.gov>, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else’s Social Security number; date of birth; driver’s license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any “trade secret or any commercial or financial information which . . . is privileged or confidential” – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled “Confidential,” and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at <http://www.ftc.gov> to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission’s privacy policy, including routine uses permitted by the Privacy Act, see <https://www.ftc.gov/site-information/privacy-policy>.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Tapplock, Inc. ("Tapplock" or "Respondent").

The proposed consent order ("proposed order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

Tapplock is a Canadian Internet of Things ("IoT") company that, among other things, sells Internet-connected, fingerprint-enabled padlocks ("smart locks") to U.S. consumers. The company advertises to U.S. consumers through its website, *www.tapplock.com*, and has previously advertised through the online crowd-funding website Indiegogo.com. 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.

In June 2018, security researchers identified critical physical and electronic vulnerabilities with Respondent's smart locks. With respect to physical security, some of Respondent's smart locks could be opened within a matter of seconds, simply by unscrewing the back panel. With respect to electronic security, one vulnerability in Respondent's API could have been exploited 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. Because Respondent failed to encrypt the Bluetooth

communication between the lock and the app, a second vulnerability could have allowed a bad actor to lock and unlock any nearby Tapplock smart lock. Finally, a third vulnerability prevented users from effectively revoking access to their smart lock once they had provided other users access to that lock.

The Commission's proposed two-count complaint alleges that Respondent violated Section 5(a) of the Federal Trade Commission Act. The first count alleges that Respondent misrepresented to consumers that their smart locks were secure. Contrary to this claim, as described above, Respondent's locks were not secure.

The second count alleges that Respondent deceived consumers about its data security practices by falsely representing that it took reasonable precautions and followed industry best practices to protect the personal information provided by consumers. Contrary to this claim, the proposed complaint alleges that Respondent failed to take reasonable precautions and follow industry best practices. For example, the proposed complaint alleges that Respondent: (1) 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; (2) 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; (3) failed to adopt and implement written data security standards, policies, procedures, or practices; and (4) failed to implement adequate privacy and security guidance or training for its employees responsible for designing, testing, overseeing, and approving software specifications and requirements.

The proposed order contains provisions designed to prevent Respondent from engaging in the same or similar acts or practices in the future. Part I of the proposed order prohibits Respondent from misrepresenting the extent to which it maintains and protects: (1) the security of a Covered Device; or (2) the privacy, security, confidentiality, or integrity of Personal Information.

Part II of the proposed order requires Respondent to establish and implement, and thereafter maintain, a comprehensive security program ("Security Program") that that protects: (1) the security of Covered Devices; and (2) the security, confidentiality, and integrity of Personal Information.

Part III of the proposed order requires Respondent to obtain initial and biennial data security assessments for twenty years.

Part IV of the proposed order requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part II.

Part V of the proposed order requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Parts VI through IX of the proposed order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to

monitor compliance. Part X states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

By direction of the Commission.

April J. Tabor,

Acting Secretary.

[FR Doc. 2020-07499 Filed: 4/8/2020 8:45 am; Publication Date: 4/9/2020]