**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of Tapplock, Inc.*, File No. 192 3011**

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 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 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.