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 **TAPPLOCK, INC., a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-4718**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

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

2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

1. "Covered Device" means (a) any computing device sold by Respondent that operates using an operating system, including any smart lock, smartphone, tablet, wearable, sensor, or any peripheral of any portable computing device; and (b) the software used to access, operate, manage, or configure a device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or sold by Respondent, directly or indirectly.

2. "Covered Incident" means any instance in which (a) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (b) Respondent discovers that Covered Devices or Personal Information necessary to access such Covered Devices (such as a key code) were, or are reasonably believed to have been, accessed without authorization.

3. "Personal Information" means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town, or other information about the location of the individual, including but not limited to fine or coarse location or GPS coordinates; (c) an email address; (d) a persistent identifier for computers or mobile devices, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, or a processor serial number; (e) a date of birth; (f) photograph; and (g) key code used to control access to a Covered Device.

4. "Respondent" means Tapplock, Inc., and its successors and assigns.

Provisions

I. Prohibition against Misrepresentations about Privacy and Security

IT IS ORDERED that Respondent, Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication, the extent to which Respondent maintains and protects: (1) the security of a Covered Device; or (2) the privacy, security, confidentiality, or integrity of Personal Information.

II. Mandated Device Security and Information Security Program

IT IS FURTHER ORDERED that Respondent must not transfer, sell, share, collect, maintain, or store Personal Information or manufacture or sell Covered Devices unless it establishes and implements, and thereafter maintains, a comprehensive Security Program ("Security Program") that protects: (1) the security of Covered Devices; and (2) the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Security Program;

B. Provide the written program and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Security Program at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the Security Program;

D. Assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks to the security of Covered Devices and to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security of Covered Devices and to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision II.D. Each safeguard must be based on (1) the sensitivity of the Covered Device's function, and (2) the volume and sensitivity of the Personal Information that is

at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Such safeguards must also include:

1. Training of all of Respondent's employees, at least once every 12 months, on how to safeguard Personal Information;

2. Technical measures to monitor all of Respondent's networks, Covered Devices, and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks; and

3. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) restricting inbound connections to approved IP addresses, (b) requiring authentication to access them, and (c) limiting employee access to what is needed to perform that employee's job function.

F. Assess, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security of Covered Devices and the security, confidentiality, or integrity of Personal Information, and modify the Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, and modify the Security Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network once every four months and promptly (not to exceed 30 days) after a Covered Incident; and (2) penetration testing of Respondent's network at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Devices and Personal Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Devices and Personal Information; and

I. Evaluate and adjust the Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Part II.D., or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Security Program. At a minimum, Respondent must evaluate the Security Program at least once every 12 months and modify the Security Program based on the results.

III. Device and Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Device Security and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Security Program; and (3) retains all documents relevant to each Assessment for five years after completion of such Assessment and provides such documents to the Commission within ten days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two year period thereafter for 20 years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period,: (1) determine whether Respondent has implemented and maintained the Security Program required by Provision II of this Order, titled Mandated Device Security and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions II.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Security Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor and must state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by Respondent's management. To the extent that Responded revises, updates, or adds one or more safeguards required under Part II of this Order in the middle of an Assessment period, the Assessment shall assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Tapplock, FTC File No. 192 3011, Docket No. C-4718." All subsequent biennial Assessments must be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten days of request.

IV. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Device and Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege; and

B. Not withhold any material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Security Program required by Provision II of this Order, titled Mandated Device Security and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-I; or (3) identification of any gaps or weaknesses in the Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of a Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Tapplock, Inc., FTC File No. 192 3011, Docket No. C-4718."

VI. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 20 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives with responsibilities related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in Provision VII of this Order titled Compliance Reports and Notices. Delivery must occur within ten days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

VII. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (2) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (5) provide a copy of each

Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Tapplock, Inc., FTC File No. 192 3011, Docket No. C-4718."

VIII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for five years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information or the security of any Covered Device, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, confidentiality, security, or integrity of Personal Information or the security of Covered Devices;

F. For five years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

G. For five years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondent's compliance with this Order;

H. For five years from the date created or received, all records, whether prepared by or on behalf of Respondent, that tend to show any lack of compliance by Respondent with this Order; and

I. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

IX. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within ten days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

X. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate May 18, 2040, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Acting Secretary

SEAL:
ISSUED: May 18, 2020