1723025

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman
Maureen K. Ohlhausen
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter

Findings

1. The Respondents are:

    a.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as

F. “Respondents” means Corporate Respondent and Individual Respondent, individually, collectively, or in any combination.

1.

A. The designation of an employee or employees to coordinate and be responsible for the Information Security Program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the security, confidentiality, and integrity of Personal Information that could result in the unintentional exposure of such information or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;

D. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security techniques;

E. Regular monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

F. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding Personal Information they receive from Respondents, and requiring such service providers, by contract, to implement and maintain appropriate safeguards; and

G. The evaluation and adjustment of the Information Security Program in light of sub-provisions E-F, any changes to Respondents' operations or business arrangements, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program.

III. Data Security Assessments by a Third Party

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

A. The Assessments must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Internet-accessible consumer-grade devices;

or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection.

B. 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 2 year period thereafter for 20 years after issuance of the Order for the biennial Assessments.

C. Each Assessment must:

1. Set forth the administrative, technical, and physical safeguards that Respondents have implemented and maintained during the reporting period;

2. Explain how such safeguards are appropriate to Respondents' size and complexity, the nature and scope of Respondents' activities, and the sensitivity of the Covered Device's function or the Personal Information;

3. Explain how the safeguards that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Data Security Program; and

4. Certify that Respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices and the privacy, security, confidentiality, and integrity of Personal Information is protected and has so operated throughout the reporting period.

D.

V. Acknowledgments of the Order

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

A. Each Respondent, within 10 days after the effective date of this Order, must submit to the

2.

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Corporate Respondent and Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a majority owner or controls directly or indirectly, must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, 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 and refund requests, whether received directly or indirectly, such as through a third party, and any response;

D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;

E. A copy of each widely disseminated representation by Respondents that describes the extent to which it uses or maintains any Personal Information, or protects the privacy, confidentiality, security, or integrity of any Personal Information and the extent to which consumers may exercise control over the collection, use, or disclosure of Personal Information; and

F. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such communication relates to Respondents

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.

Donald S. Clark
Secretary

SEAL:
ISSUED: September 6, 2018