[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 162 3130]

InfoTrax Systems, L.C. and Mark Rawlins; 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: "InfoTrax Systems, L.C. and Mark Rawlins; File No. 162 3130" 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: Andrea Arias (202-326-2715), 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 Home Page (for November 12, 2019), on the World Wide Web, at 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 "InfoTrax Systems, L.C. and Mark Rawlins; File No. 162 3130" 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.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online through the https://www.regulations.gov website.

If you prefer to file your comment on paper, write "InfoTrax Systems, L.C. and Mark Rawlins; File No. 162 3130" 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 that 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 that your comment does not include any 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 InfoTrax Systems, L.C. ("InfoTrax") and Mark Rawlins (collectively "Respondents").

The proposed consent order ("proposed order") has been placed on the public record for thirty (30) days for receipt of comments from interested persons. Comments received during this period will become part of the public record. After thirty (30) days,

the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

This matter involves InfoTrax, a technology company that provides backend operations systems and online distributor tools for the direct sales industry. Respondents have stored personal information about more than eleven million consumers.

The Commission's proposed complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act ("FTC Act"). The proposed complaint alleges that Respondents engaged in a number of unreasonable security practices and that, as a result of these practices, an intruder, or intruders, were able to gain unauthorized access to consumers' personal information in March 2016. During multiple breaches, intruder(s) accessed and/or downloaded the personal information of over one million consumers. The types of information exposed included full names; physical addresses; email addresses; telephone numbers; Social Security Numbers ("SSNs") or other government identification numbers; clients' distributors' user IDs and passwords; admin IDs and passwords; payment card information including credit or debit card numbers, Card Verification Values ("CVVs") and expiration dates; and bank account information including bank account and routing numbers. (However, a particular individual's record does not necessarily contain every one of these data types.)

The proposed complaint alleges that Respondents:

- Failed to have a systematic process for inventorying and deleting consumers' personal information stored on InfoTrax's network that is no longer necessary;

- Failed to adequately assess the cybersecurity risk posed to consumers' personal information stored on InfoTrax's network by performing adequate code review of InfoTrax's software, and penetration testing of InfoTrax's network and software;
- Failed to detect malicious file uploads by implementing protections such as adequate input validation;
- Failed to adequately limit the locations to which third parties could upload unknown files on InfoTrax's network;
- Failed to adequately segment InfoTrax's network to ensure that one client's distributors could not access another client's data on the network;
- Failed to implement safeguards to detect anomalous activity and/or cybersecurity events. For example, Respondents failed to: (1) implement an intrusion prevention or detection system to alert Respondents of potentially unauthorized queries and/or access to InfoTrax's network; (2) use file integrity monitoring tools to determine whether any files on InfoTrax's network had been altered; and (3) use data loss prevention tools to regularly monitor for unauthorized attempts to exfiltrate consumers' personal information outside InfoTrax's network boundaries; and
- Stored consumers' personal information, including consumers' SSNs, payment card information (including full or partial credit card and debit card numbers, CVVs, and expiration dates), bank account information (including account and routing numbers), and authentication credentials

such as user IDs and passwords, in clear, readable text on InfoTrax's network.

The proposed complaint alleges that Respondents could have addressed each of the failures described above by implementing readily available and relatively low-cost security measures.

The proposed complaint alleges that Respondents' failure to employ reasonable data security practices to protect personal information—including names, addresses, SSNs, other government identifiers, and financial account information—caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Respondents' failure to employ reasonable data security practices constitutes an unfair act or practice under Section 5 of the FTC Act.

The proposed order contains injunctive provisions addressing the alleged unfair conduct. Part I of the proposed order prohibits each Covered Business from transferring, selling, sharing, collecting, maintaining, or storing personal information unless each Covered Business establishes and implements, and thereafter maintains, a comprehensive information security program that protects the security, confidentiality, and integrity of such personal information.[1]

Part II of the proposed order requires Respondents to obtain initial and biennial data security assessments for twenty (20) years.

---

[1] "Covered Business" includes InfoTrax; any business that InfoTrax controls, directly or indirectly; and any business that Mr. Rawlins controls, directly or indirectly, except for the businesses that own, lease, and/or operate a campground in Bunkerville, Nevada, and solely to the extent that the businesses are engaged in the operation of that campground.

Part III of the proposed order requires Respondents to disclose all material facts to the assessor; prohibits Respondents from misrepresenting any fact material to the assessments required by Part II; and requires Respondents to provide or otherwise make available to the assessor all information and material that is relevant to the assessment for which there is no reasonable claim of privilege.

Part IV requires Respondents to submit an annual certification from a senior corporate manager (or senior officer of each Covered Business responsible for each Covered Business's information security program) that: (1) each Covered Business has implemented the requirements of the Order; (2) each Covered Business is not aware of any material noncompliance that has not been corrected or disclosed to the Commission; and (3) includes a brief description of any covered incident involving unauthorized access to or acquisition of personal information.

Part V requires Respondents to submit a report to the Commission of the discovery of any covered incident.

Parts VI through IX of the proposed order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part X states that the proposed order will remain in effect for twenty (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.

Joel Christie,

Acting Secretary.

[FR Doc. 2019-25109 Filed: 11/19/2019 8:45 am; Publication Date: 11/20/2019]