1623130

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	**DECISION AND ORDER**
INFOTRAX SYSTEMS, L.C., a limited liability company, and	**DOCKET NO. C-**
MARK RAWLINS	

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents 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 Respondents with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit 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 Respondents have 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 thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. 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 Respondents are:

   a. Respondent InfoTrax Systems, L.C. ("InfoTrax"), a limited liability company with its principal office or place of business at 1875 South State Street, Suite 3000, Orem, Utah 84097.

   b. Respondent Mark Rawlins, founder and Chief Executive Officer of Corporate Respondent InfoTrax Systems, L.C. during the time period relevant to the Complaint. Individually or in concert with others, he formulated, directed, or controlled the policies, acts, or practices of InfoTrax Systems, L.C. His principal office or place of business is in Orem, Utah.

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

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Business" means: (1) Corporate Respondent; (2) any business that Corporate Respondent controls, directly or indirectly; and (3) any business that Individual Respondent controls, directly or indirectly, except for the businesses that own, lease, and/or operate the Aravada Springs Campground ("Campground"), located in Bunkerville, Nevada, solely to the extent that the businesses are engaged in the operation of the Campground.

B. "Covered Incident" means any instance in which any United States federal, state, or local law or regulation requires a Covered Business or Individual Respondent, or any client of a Covered Business, to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by a Covered Business from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.

C. "Personal Information" means individually identifiable information from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) date of birth; (6) a Social Security number; (7) driver's license or other government issued identification number; (8) financial institution account number; (9) credit or debit card information; (10) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; and (11) authentication credentials such as a user ID and password.

D. "Respondents" means Corporate Respondent and Individual Respondent, individually, collectively, or in any combination.

1. "Corporate Respondent" means InfoTrax, and its successors and assigns.

2. "Individual Respondent" means Mark Rawlins.

Provisions

I. Mandated Information Security Program

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, each Covered Business must, at a minimum:

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

B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its Information Security Program at least once every twelve (12) months and promptly after a Covered Incident;

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

D. Assess and document, at least once every twelve (12) months and promptly following a Covered Incident, internal and external risks 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 the internal and external risks to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision I.D. Each safeguard shall be based on 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. Corporate Respondent's safeguards shall also include:

1. Policies, procedures, and technical measures to systematically inventory Personal Information stored on Corporate Respondent's network and delete Personal Information that is no longer necessary;

2. Measures to assess the cybersecurity risk posed by Corporate Respondent's code to Personal Information stored on Corporate Respondent's network, including, at least once every twelve (12) months and promptly after a Covered Incident: (a) software code review; and (b) penetration testing of Corporate Respondent's software;

3. Technical measures to detect unknown file uploads, such as input validation;

4. Technical measures to limit the locations to which third parties can upload files on Corporate Respondent's network;

5. Segmentation of Corporate Respondent's network to ensure that one client's distributors cannot access another client's data on Corporate Respondent's network;

6. Technical measures to detect anomalous activity and/or cybersecurity events on Corporate Respondent's network, including (a) an intrusion prevention or detection system to alert Corporate Respondent of potentially unauthorized queries and/or access to its network; (b) file integrity monitoring tools to determine whether files on Corporate Respondent's network have been altered; and (c) data loss prevention tools to regularly monitor for unauthorized attempts to exfiltrate Personal Information outside Corporate Respondent's network boundaries; and

7. Encryption of Social Security numbers, payment card information (including full credit card and debit card numbers, Card Verification Values, and expiration dates), bank account information (including account and routing numbers), and authentication credentials such as user IDs and passwords on Corporate Respondent's network.

F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly following a Covered Incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of each of Respondents' network(s) once every four months and promptly after a Covered Incident, and penetration testing of each of the Covered Business's network(s) at least once every twelve (12) months and promptly after a Covered Incident;

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

I. Evaluate and adjust the Information Security Program in light of any changes to its operations or business arrangements, a Covered Incident, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, each Covered Business must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

II. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision I of this Order titled Mandated Information Security Program, Respondents 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 Information Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) 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, Respondents shall 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 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must: (1) determine whether each Covered Business has implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of each Covered Business's implementation and maintenance of sub-Provisions I.A-I; (3) identify any gaps or weaknesses in the Information 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 a Covered Business's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by a Covered Business's management.

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Assessment to the Commission within ten (10) 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 InfoTrax Systems, L.C. and Mark Rawlins, FTC File No. 1623130." All subsequent biennial Assessments shall be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

III. Cooperation with Third Party Information Security Assessor

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

A. Disclose all 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 Respondents have implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions I.A-I; or (3) identification of any gaps or weaknesses in the Information Security Program; and

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

IV. Annual Certification

IT IS FURTHER ORDERED that, in connection with compliance with Provision I of this Order titled Mandated Information Security Program, Respondents shall:

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 each Covered Business responsible for each Covered Business's Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business 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 any 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, "In re InfoTrax Systems, L.C. and Mark Rawlins, FTC File No. 1623130."

V. Covered Incident Reports

IT IS FURTHER ORDERED that Respondents, for any Covered Business, within a reasonable time after the date of discovery of a Covered Incident, but in any event no later than ten (10) days after the date the Covered Business, or any of the Covered Business's clients, first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports 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, "In re InfoTrax Systems, L.C. and Mark Rawlins, FTC File No. 1623130."

VI. Acknowledgments of the Order

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

A. Each Respondent, within ten (10) 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 twenty (20) years after the issuance date of this Order, Individual Respondent, for any Covered Business that Individual Respondent, individually or collectively with any other Respondents, is the majority owner or controls directly or indirectly, and Corporate Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision VII of this Order titled Compliance Report and Notices. Delivery must occur within ten (10) 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 a Respondent delivered a copy of this Order, that Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

VII. Compliance Report and Notices

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

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:

1. Each Respondent must: (a) 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; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if he knows or should know due to his own involvement); (d) 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 (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, Individual Respondent must: (a) identify all his telephone numbers and all his physical, postal, email and Internet addresses, including all residences; (b) identify all his business activities, including any business for which such Respondent

performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; and (c) describe in detail such Respondent's involvement in each such business activity, including title, role, responsibilities, participation, authority, control, and any ownership.

B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:

1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of any Corporate 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.

2. Additionally, Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Individual Respondent performs services whether as an employee or otherwise and (ii) any entity in which Individual Respondent has any ownership interest and over which Individual Respondent has direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (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, "In re InfoTrax Systems, L.C., and Mark Rawlins, FTC File No. 1623130."

VIII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years, unless otherwise specified below. Specifically, Corporate Respondent and Individual

Respondent, for any Covered Business that Individual Respondent, individually or collectively with any other Respondent, 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, the costs incurred in generating those revenues, and resulting net profit or loss;

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 concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. For five (5) 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 Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

E. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondents' compliance with this Order;

F. For five (5) years from the date created or received, all records, whether prepared by or on behalf of Respondents, that tend to show any lack of compliance by Respondents with this Order; and

G. 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 Respondents' compliance with this Order:

A. Within ten (10) days of receipt of a written request from a representative of the Commission, each 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 each Respondent. Respondents must permit representatives

of the Commission to interview anyone affiliated with any 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 Respondents or any individual or entity affiliated with Respondents, 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 twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (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 twenty (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: