## 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

INFOTRAX SYSTEMS, L.C., a limited liability company, and

MARK RAWLINS

DECISION AND ORDER DOCKET NO. C-4696

DE

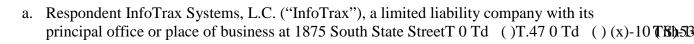
present the draft Complaint to the Commission for its consideral Commission, the draft Complaint would charge the Respondent Trade Commission Act, 15 U.S.C. § 45(a).

Respondents and BCP thereafter executed an Agreeme ("Consent Agreement"). The Consent Agreement includes: (1) they neither admit nor demany of the allegations in the Complain in this Decision and Order, and that only for purposes of this acreessary to establish jurisdiction; and (2) waivers and other pr Commission's Rules.

The Commission considered the matter and determined Respondents have violated the Federal Trade Commission Act.

## Findings

	1.	The	Res	pond	lents	are
--	----	-----	-----	------	-------	-----



D.	"Respondent'smeans	s Corporate Responde	nt and	Individual	Respondent,	individually,
	collectively, or in any	y combination.				

1. "Corporate RespondentheansInfoTrax, and its successors and assigns.

2.

- 2. Measures to assess the cybersecurity risk plays control of the Personal Information stored on Corporate Respondent's network, incladings once every twelve (12) months and promptly after a Covered Inc (de) is to fit ware code review and (b) penetration testing Corporate Respondent's of tware;
- 3. Technical measures to detectknown file uploads, such as input validation;
- Technical measures to limit the cations to which third parties an upload files on Corporate Respondent's network;
- 5. Segmenation of Corporate Respondent's network to ensure that one client's distributorscannot access another client's data on Corporate pondent's network;
- 6. Technical measures detect anomalous activity and/or cybersecurity events on CorporateRespondent's network, including (a) intrusion prevention or detection system to alert Corporatespondent of potentially unauthorized queries and/or access to its network; (b) integrity monitoring tools to determine whether files on Corporate Respondent's network have been altered (c) data loss prevention tools to regularly monitor for unauthorized attempts to exfilt the sonal information outside Corporate Respondent's network boundaries; and
- 7. Encryption of Social Security numbers, payment card information (including full credit card and debit cardumbers, Card Verification Values, and expiration dates), bank account information (including account and routing numbers), and authentication credentials such as uberand 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 addresssks to the security, confidentiality, or integrity of Personal Information, and modify the Imfation Security Program based on the results;
- Las o4 (e)fTJ 0 Tc 0 Tw -32.44 (I)15 Td [(P)-3 (e)-6 4pondentl(s2)3 j EMCc 0 Tw -32 (7Td [(nu G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) mon nGTo4 (nd nd m)-2 (odi)-2 (f)-7 (y)20J 0 Tc 0 oiin aexed

NW, Washington, DC20580. The subject line must begitn fe InfoTraxSystems, L.C. and Mark RawlinsFTC File No.1623130, FTC Docket No. C-4696."

## 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 Consistences clients irst notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The portmust include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Coveredtlocidered;
- 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 acanesis rotect 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 the Covered Business any of its clients consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reported 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 bedjinr,e InfoTrax Systems, L. and Mark Rawlins FTC File No.1623130, FTC Docket No. C-4696."

## VI. Acknowledgments of the Order

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

A. EachRespondent, withiten (10) days after the effective datethis Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

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

1. ΟV

R

- 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 seimicelstion to any aspect of the Order, whether as an employee or otherwise, that person's name; addresses; telephone numbers; job title oposition; 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 are 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 Respondentiance 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 @der;
- 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 this Order; and
- G. All records necessary to demonstrate full compliance with **Proxi**sion of this Order, including all submissions to the Commission.

IX. Compliance Monitoring

IT IS FURTHER ORDs' o-iat-1 9(o)-1ie.DC -0..57 -ie.DC -0.0rte fsioe th laod cng(uc)4 (s)-1 (per land) (per lan