**1623130**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

| | |
|---|---|
| **COMMISSIONERS:** | **Joseph J. Simons, Chairman**<br>**Noah Joshua Phillips**<br>**Rohit Chopra**<br>**Rebecca Kelly Slaughter**<br>**Christine S. Wilson** |

| | | |
|---|---|---|
| **In the Matter of**<br><br>**INFOTRAX SYSTEMS, L.C., a limited liability company, and**<br><br>**MARK RAWLINS** | ) | **DOCKET NO.** |

# COMPLAINT

The Federal Trade Commission ("Commission" or "FTC"), having reason to believe that InfoTrax Systems, L.C., a limited liability company, and Mark Rawlins, individually and as founder and Chief Executive Officer of InfoTrax Systems, L.C. (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. Respondent Mark Rawlins ("Mr. Rawlins") is the founder of InfoTrax and served as Chief Executive Officer of InfoTrax during the time period relevant to this complaint. Prior to founding InfoTrax in 1998, Mr. Rawlins spent eighteen years at a software company, and he studied computer science in college. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of InfoTrax, including the acts and practices alleged in this complaint. Specifically, Mr. Rawlins reviewed and approved InfoTrax's information technology security policies, was involved in discussions with clients about data security regularly, and was involved in the company's long-term data security strategy. His principal office or place of business is in Orem, Utah.

3. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

## RESPONDENTS' BUSINESS PRACTICES

4. Since 1998, Respondents have operated a technology company that provides backend operations systems and online distributor tools for the direct sales industry.

5. InfoTrax's clients are primarily multi-level marketers, which rely on InfoTrax's products and services to manage all aspects of their business operations, including compensation, inventory, orders, accounting, training, communication, and data security, among other things. InfoTrax's clients include multi-level marketers like dōTERRA International, LLC ("dōTERRA"), XanGo, LLC ("XanGo"), and LifeVantage Corp. ("LifeVantage").

6. Typically, InfoTrax operates the major aspects of its clients' website portals for their distributors and customers. Through these website portals, individuals register with multi-level marketers as distributors, place orders for themselves and the end consumers who purchase from them, and enroll new distributors.

7. In the process of registering and placing orders, distributors—on behalf of themselves and their end consumers—supply InfoTrax with significant amounts of personal information about themselves and their end consumers, which may include full names; dates of birth; physical and email addresses; telephone numbers; Social Security numbers ("SSNs") or other government identification numbers; payment card information including credit or debit card numbers, Card Verification Values ("CVVs") and expiration dates; bank account information including bank account and routing numbers; and account user IDs and passwords.

8. As part of providing products and services to manage the business operations of its clients, InfoTrax assumes responsibility for the security and confidentiality of consumers' personal information by contract, and purports to ensure that all personal information is adequately protected.

9. As of September 2016, Respondents stored personal information for approximately 11.8 million consumers.

## RESPONDENTS' UNREASONABLE DATA SECURITY PRACTICES

10. From at least 2014 through March 2016, Respondents engaged in a number of unreasonable data security practices. Among other things, Respondents:

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

b. 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;

c. failed to detect malicious file uploads by implementing protections such as adequate input validation;

d. failed to adequately limit the locations to which third parties could upload unknown files on InfoTrax's network;

e. failed to adequately segment InfoTrax's network to ensure that one client's distributors could not access another client's data on the network;

f. failed to implement safeguards to detect anomalous activity and/or cybersecurity events. For example, Respondents failed to:

i. implement an intrusion prevention or detection system to alert Respondents of potentially unauthorized queries and/or access to InfoTrax's network;

ii. use file integrity monitoring tools to determine whether any files on InfoTrax's network had been altered; and

iii. use data loss prevention tools to regularly monitor for unauthorized attempts to exfiltrate consumers' personal information outside InfoTrax's network boundaries; and

g. 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.

11. Respondents could have addressed each of the failures described in paragraph 10 by implementing readily available and relatively low-cost security measures.

## SECURITY INCIDENTS AND DATA BREACHES

12. As a result of the failures described in paragraph 10, on or before May 5, 2014, an intruder exploited vulnerabilities in InfoTrax's server and a client's website to upload malicious code that enabled remote control over InfoTrax's server. Using the code, an intruder could view files on InfoTrax's server, delete such files, upload new files, and access data from the server.

13. During a period of almost two years, between May 5, 2014, and February 23, 2016, an intruder accessed InfoTrax's server undetected a total of seventeen times.

14. Thereafter, on March 2, 2016, an intruder began to pull information from InfoTrax's systems. Specifically, the intruder queried certain databases on InfoTrax's systems from which the intruder accessed personal information of approximately one million consumers, including: full names; physical addresses; email addresses; telephone numbers; SSNs; distributor user IDs and passwords; and admin IDs and passwords. One of these databases contained legacy data that Respondents failed to migrate to a new product. Because Respondents did not properly inventory and manage this data, they did not know this data existed, much less take steps to protect it.

15. On that same day, an intruder accessed a different log file stored on InfoTrax's server that contained, among other things, even more personal information of consumers, including over 600 names and addresses, over 150 SSNs or other government identification numbers, over 500 unique unmasked payment account numbers with expiration data and CVVs, and 16 bank account and routing numbers.

16. On March 6, 2016, an intruder queried yet another database from which the intruder accessed over 4100 user IDs and passwords of distributors, in clear text, which could be used to access a client's website. With these user IDs and passwords, the intruder could access those distributors' accounts, where the intruder could access some of the personal information of those distributors and their end consumers, as well as personal information from other websites where distributors and their end consumers used the same user IDs and passwords.

17. Because Respondents failed to implement safeguards and security measures to detect anomalous activity and/or cybersecurity events, Respondents did not discover the presence of the intruder(s) from May 5, 2014, until March 7, 2016, when InfoTrax began receiving alerts that one of its servers had reached its maximum capacity. The only reason Respondents received any alerts is because an intruder had created a data archive file that had grown so large that the disk ran out of space. Only then did Respondents begin to take steps to remove the intruder from InfoTrax's network.

18. On March 14, 2016, an intruder compromised Respondents' environment again, using malicious code to collect information through a client's website portal operated by Respondents. The code was designed to harvest payment card and other billing data newly submitted by distributors during the checkout process. The intruder thus obtained over 2300 unique, full payment card numbers—including names, physical addresses, CVVs, and expiration dates.

19. On March 29, 2016, an intruder used the user ID and password of a valid distributor account to upload more malicious code. The intruder introduced this code through the web portal of one InfoTrax client, but the intruder was still able to access another client's environment because the intruder's malicious code gave the intruder elevated access. The intruder then uploaded malicious code to collect information from that client's website again, including newly submitted full names, payment card numbers, expiration dates, and CVVs.

## INJURY TO CONSUMERS AND BUSINESSES

20. Breached personal information, such as that stored in InfoTrax's system, is often used to commit identity theft and fraud. For example, identity thieves use stolen names, addresses, and SSNs to apply for credit cards in the victim's name. When the identity thief fails to pay credit card bills, the victim's credit suffers. InfoTrax's breaches affected distributors and end consumers for several multi-level marketers, including dōTERRA, XanGo, and LifeVantage.

21. Similarly, stolen financial information, such as credit card numbers, expiration dates, and security codes that InfoTrax holds, can be used to commit fraud. Specifically, a thief could make unauthorized purchases using stolen credit card information.

22. As of September 2016, AllClear ID, Inc. ("AllClear"), the third-party call center retained by one InfoTrax client to assist with breach response, had received over 280 reports of alleged fraud from that client's distributors and end consumers, including 238 complaints of unauthorized credit card charges, 34 complaints of new credit lines opened, 15 complaints of tax fraud, and 1 complaint of misuse of information for employment purposes. In addition, that client received reports of potential fraud from approximately 22 distributors and end consumers.

23. Even if identity theft and fraud do not occur immediately after a breach, a breach of personal information such as that stored in InfoTrax's system makes identity theft and fraud likely.

24. The breaches of personal information imposed costs, such as handling breach response communications, identifying affected consumers, and responding to consumer complaints, on some of InfoTrax's clients. InfoTrax notified all of its clients of the breaches so they could respond appropriately. For example, between March 2016 and April 2016, one InfoTrax client sent out breach notifications to payment card networks, banks, credit reporting agencies, law enforcement, state regulators, distributors, and end consumers, and it hired counsel and security experts to investigate the breaches.

25. Respondents' failure to provide reasonable security for the personal information of distributors and end consumers has caused or is likely to cause substantial injury to consumers in the form of fraud, identity theft, monetary loss, and time spent remedying the problem.

26. Distributors and end consumers had no way of independently knowing about Respondents' security failures and could not reasonably have avoided possible harms from such failures.

## VIOLATION OF THE FTC ACT

### Count 1 – Unfairness: Failure to Employ Reasonable Data Security Practices

27. As described in Paragraphs 10 to 26, 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. This practice was, and is, an unfair act or practice.

28. The acts and practices of Respondents as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

**THEREFORE**, the Federal Trade Commission this __ day of _________ 2019, has issued this complaint against Respondents.

By the Commission.

April J. Tabor
Acting Secretary

SEAL:
ISSUED: