162 3130

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

Ss
R2(. Wi),i

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 G À 7 (5 5 , Q W H U Q D W L R Q D O / / &
° À R PNE ± Ð D IvÀ Â D ` À L Ôü D ädÄ" I h‘ð À !Á'oÀ ! NFB"r ì¡7L¶ÍP58 I9-6 (c)4 p10 (, c)4 (

information stored on InfoTrax's

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 as it was submitted by distributors during the checkout process. The intruder 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