Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of* InfoTrax Systems, L.C. and Mark Rawlins**
File No. 1623130

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 by 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.