112 3143

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen

In the Matter of **EPN, Inc., also d/b/a Checknet, Inc. a corporation.**	**DOCKET NO. C-4370**

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that EPN, Inc., d/b/a Checknet Inc. ("EPN") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent EPN is a Utah corporation with its principal office or place of business at 746 East 1910 South, Suite 3, Provo, UT 84606.

2. The acts and practices of Respondent as alleged in this complaint are in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. At all relevant times, Respondent has been in the business of collecting debts for clients in a variety of industries, including commercial credit, retail, and healthcare.

4. In conducting business, Respondent routinely obtains information about its clients' customers. This information includes, but is not limited to: name, address, date of birth, gender, Social Security number, employer address, employer phone number, and in the case of healthcare clients, physician name, insurance number, diagnosis code, and medical visit type (collectively, "personal information").

5. Respondent operates computer networks in conducting its business. Among other things, it uses the networks to receive, store, and use personal information about its clients' customers to assist in collecting debts on its clients' behalf.

EPN'S SECURITY PRACTICES

6. EPN has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks. Among other things, Respondent failed to:

   (a) Adopt an information security plan that was appropriate for its networks and the personal information processed and stored on them. For example, EPN did not have an incident response plan;

   (b) Assess risks to the consumer personal information it collected and stored online;

   (c) Adequately train employees about security to prevent unauthorized disclosure of personal information;

   (d) Use reasonable measures to assess and enforce compliance with its security policies and procedures, such as scanning networks to identify unauthorized peer-to-peer ("P2P") file sharing applications and other unauthorized applications operating on the networks or blocking installation of such programs; and

   (e) Use reasonable methods to prevent, detect, and investigate unauthorized access to personal information on its networks, such as by adequately logging network activity and inspecting outgoing transmissions to the Internet to identify unauthorized disclosures of personal information.

7. As a result of the failures set forth in Paragraph 6, EPN's chief operating officer was able to install a P2P application on her desktop computer, which was connected to EPN's computer network. Respondent is unaware of the date the application was installed; it was disabled in April 2008 when EPN was informed by a client that two files containing personal information about the client's debtors were available on a P2P network ("breached files"). EPN had no business need for the P2P application.

8. The breached files contained personal information about approximately 3,800 consumers, including each consumer's name, address, date of birth, Social Security number, employer name, employer address, health insurance number, and a diagnosis code. Such information, among other things, can easily be used to facilitate identity theft (which also could result in medical histories that are inaccurate because they include the medical records of identity thieves) and exposes sensitive medical data.

9. The breached files were shared to the P2P network from EPN's chief operating officer's computer, and other files containing personal information may have been shared to P2P networks from that computer.

10. Files shared to a P2P network are available for viewing or downloading by anyone using a personal computer with access to the network. Generally, a file that has been shared cannot be permanently removed from P2P networks.

VIOLATION OF THE FTC ACT

11. As set forth in Paragraphs 6 through 10, Respondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. Therefore, Respondent's practices were, and are, an unfair act or practice.

12. The acts and practices of Respondent as alleged in this Complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this third day of October, 2012, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary