Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of EPN, Inc., File No. 112 3143

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from EPN, Inc.

The proposed consent 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.

The Commission's proposed complaint alleges that EPN, which does business as Checknet, Inc., is a Utah corporation that is in the business of collecting debts for clients in a variety of industries, including commercial credit, retail, and healthcare. According to the complaint, In conducting business, EPN routinely obtains information about its clients' customers, which 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.

The complaint further alleges that EPN engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks. In particular, EPN failed to: (1) adopt an information security plan that was appropriate for its networks and the personal information processed and stored on them; (2) assess risks to the consumer personal information it collected and stored online; (3) adequately train employees about security to prevent unauthorized disclosure of personal information; (4) 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 (5) 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.

The complaint alleges that as a result of these failures, an EPN employee was able to install a P2P application on her desktop computer, which was connected to EPN's computer network, resulting in two files containing personal information about a client's customers being made available on a P2P network; other files containing personal information may also have been shared to P2P networks from that computer. 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. The complaint alleges that 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.

In fact, the presence of P2P software on business computers can pose significant data security risks. A 2010 FTC examination of P2P-related breaches uncovered a wide range of sensitive consumer data available on P2P networks, including health-related information, financial records, and drivers' license and social security numbers. *See* Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), http://www.ftc.gov/opa/2010/02/p2palert.shtm. Files shared to a P2P network are available for viewing or downloading by any computer user with access to the network. Generally, a file that has been shared cannot be removed permanently from the P2P network. In addition, files can be shared among computers long after they have been deleted from the original source computer.

According to the complaint, EPN'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, EPN's practices were, and are an unfair act or practice, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45(a).

The proposed order contains provisions designed to prevent EPN from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits misrepresentations about the privacy, security, confidentiality, and integrity of any personal information collected from or about consumers. Part II of the proposed order requires EPN to establish, implement, and thereafter maintain a comprehensive information security program, including the designation of an employee to oversee EPN's security program, employee training, and implementation of reasonable safeguards. Part III of the order requires EPN to obtain, for a period of twenty years, biennial assessments of its information security program from an independent third-party professional possessing certain credentials or certifications.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires EPN to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third party assessments and supporting documents, EPN must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that EPN submit a compliance report to the FTC within 90 days, and periodically thereafter as requested. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.