UNITED STATES OF AMERICA **112 3143**
FEDERAL TRADE COMMISSION

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

AGREEMENT CONTAINING CONSENT ORDER

certain acts and practices of EPN, Inc., also d/b/a Checknet, Inc. ("EPN" or "proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order, resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between EPN, Inc. and counsel for the Federal Trade Commission that:

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. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

   a. Any further procedural steps;

   b. The requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

   c. All rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this D(dr)Tj9.960 so0 TD3000 cm0.00 0.00 0no 0.0000 TD(dr)Tj9.9

in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "respondent" shall mean EPN, Inc., also dba Checknet, Inc., and each of their successors and assigns.

2. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) date of birth; (c) a home or other physical address, including street name and name of city or town; (d) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (e) a telephone number; (f) a Social Security number; (g) credit or debit card information, including card number, expiration date, and security code; (h) a persistent identifier, such as a customer number held in a "cookie" or processor serial number; and (i) any information that is combined with any of (a) through (h) above.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, or through any corporation, subsidiary, division, website or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers.

II.

IT IS ORDERED that respondent, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. The designation of an employee or employees to coordinate and be accountable

B. The identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. The evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by the Part II of this order; and

D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, initial and biennial Assessments shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line "In re EPN, Inc., FTC File Number 1123143." *Provided, however,* that, in lieu of overnight courier, Assessments may be sent by first-class mail, but only if an electronic version of such Assessments is contemporaneously sent to the Commission at DEBrief@ftc.gov.

Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line "In re EPN, Inc., FTC File Number 1123143." *Provided, however*, that, in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of such notices is contemporaneously sent to the Commission at DEBrief@ftc.gov.

APPROVED:

_____

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection

_____

David C. Vladeck
Director
Bureau of Consumer Protection