

Complaint

IN THE MATTER OF

EPN, INC.
D/B/A
CHECKNET, INC.

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4370; File No. 112 3143
Complaint, October 3, 2012 – Decision, October 3, 2012

This consent order addresses EPN, Inc.'s allowing an EPN employee 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. The complaint alleges that EPN violated of Section 5(a) of the Federal Trade Commission Act by failing to employ reasonable and appropriate measures to prevent unauthorized access to personal information which 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. The consent order prohibits misrepresentations about the privacy, security, confidentiality, and integrity of any personal information collected from or about consumers.

Participants

For the *Commission*: Karen Jagielski, Jessica Lyon, and Manas Mohapatra.

For the *Respondent*: Amy Purcell and Scott Vernick, Fox Rothschild LLP.

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.

Complaint

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,

Complaint

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.

Decision and Order

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.

DECISION AND ORDER

The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and

Decision and Order

does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment received from an interested person pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent, EPN, Inc., also d/b/a Checknet Inc. is a corporation organized, existing and doing business under and by virtue of the laws of the State of Utah, with its office and principal place of business located in the City of Provo, State of Utah.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

- A. Unless otherwise specified, "respondent" shall mean EPN, Inc., also dba Checknet, Inc., and each of their successors and assigns.
- B. "Personal information" shall mean individually identifiable information from or about an individual

Decision and Order

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.

- C. "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

Decision and Order

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 for the information security program.
- 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

Decision and Order

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

Decision and Order

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.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. For a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. For a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other

Decision and Order

materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that for a period of five (5) years from the date of entry of this Order, respondent shall deliver copies of the Order as directed below:

- A. Respondent must deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents and representatives who engage in conduct related to the subject matter of the Order, and (3) any business entity resulting from any change in structure set forth in Part VI. For current personnel, delivery shall be within thirty (30) days of service of this Order. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in respondent's name or address. *Provided, however,* that, with respect to any proposed change in the entity about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent

Decision and Order

shall notify the 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.

VII.

IT IS FURTHER ORDERED that respondent within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission, each report 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, reports may be sent by first-class mail, but only if an electronic version of such reports is contemporaneously sent to the Commission at DEBrief@ftc.gov.

VIII.

This order will terminate on October 3, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

Analysis to Aid Public Comment

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**COOPERATIVA DE FARMACIAS
PUERTORRIQUEÑAS**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket No. C-4374; File No. 101 0079**Complaint, November 6, 2012 – Decision, November 6, 2012*

This consent order addresses Cooperativa de Farmacias Puertorriqueñas's ("Coopharma") negotiating, entering into, and implementing agreements among its member pharmacy owners to fix the prices on which they contract with third-party payers in Puerto Rico. The complaint alleges that Coopharma's member pharmacies restrained competition by jointly negotiating and entering into agreements with third-party payers. Coopharma achieved this result by encouraging its members: (1) to refuse to deal with third-party payers except through Coopharma; and (2) to threaten termination, or actually terminate, contracts with payers that refused to deal with Coopharma on the terms it demanded. The consent order prohibits Respondent from entering into or facilitating agreements between or among any pharmacies: (1) to negotiate on behalf of any pharmacy with any payer; (2) to refuse to deal or threaten to refuse to deal with any payer; (3) to include any term, condition, or requirement upon which any pharmacy deals, or is willing to deal, with any payer, but not limited to, price terms; or (4) not to deal individually with any payer, or not to deal with any payer other than through Respondent.

Participants

For the *Commission*: Linda Blumenreich and Randy David Marks.

For the *Respondent*: David Balto, Brendan Coffman, and Brad Wasser, Law Offices of David Balto.

COMPLAINT

Pursuant to the provisions of the Federal Trade Commission Act, as amended, 15 U.S.C. § 41, et seq., and by virtue of the authority vested in it by said Act, the Federal Trade Commission ("Commission"), having reason to believe that Respondent Cooperativa de Farmacias Puertorriqueñas ("Coopharma") violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, and it appearing to the Commission that a proceeding