UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

STATE OF VERMONT

Plaintiff

v. **Civil No.** 2:11-cv-16

HEALTH NET, INC., AND
HEALTH NET OF THE NORTHEAST, INC.

Defendants

COMPLAINT

Introduction

1 Plaintiff State of Vermont, by and through Attorney General William H. Sorrell, brings this action for injunctive relief, statutory damages, attorneys fees, and costs against Defendants Health Net, Inc., and Health Net of the Northeast, Inc., under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), Pub. L. No. 111-5, 123 Stat. 226, the Vermont Consumer Fraud Act, 9 V.S.A §§ 2451-2466, and the Vermont Security Breach Notice Act, 9 V.S.A. §§ 2430-2435, and alleges as follows:

Jurisdiction and Venue

2. The Court has jurisdiction pursuant to 42 U.S.C. § 1320d-5(d)(1), 28 U.S.C. § 1331, and 28 U.S.C. § 1367

3. Plaintiff State of Vermont has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. § 1320d-5(d)(4).

4. This action is in the public interest pursuant to 9 V.S.A. § 2458(a).

5. Venue is proper in this judicial district pursuant to 28 U.S.C § 1391

Parties

6. Plaintiff State of Vermont, by and through Attorney General Sorrell, is charged, *inter alia*, with enforcement of HIPAA, 42 U.S.C. § 1320d-5(d), the Vermont Security Breach Notice Act, 9 V.S.A. § 2435(g), and the Vermont Consumer Fraud Act, 9 V.S.A § 2458.
7. Defendant Health Net, Inc., ("HN") is a publicly traded Delaware corporation with its main office located at 21650 Oxnard Street, Woodland Hills, CA 91367
8. Defendant Health Net of the Northeast, Inc., ("HNNE") is a wholly owned subsidiary of HN, with its main office located at One Far Mill Crossing, Shelton, CT 06484.
9. Defendants are and at all times relevant to this matter have been health care companies that provide health insurance plans, including Medicare prescription drug plans, to Vermont residents.
10. Defendants are and at all times relevant to this matter have been health plans within the meaning of HIPAA, 42 U.S.C. § 1320d(5) & 45 C.F.R. §160.103, and are thus "covered entities" subject to HIPAA's standards governing individually identifiable health information, specifically, the Privacy Rule, *see generally* 45 C.F.R. pts. 160 & 164.
11. Defendants are and at all times relevant hereto have been "data collectors" within the meaning of Vermont's Security Breach Notice Act, 9 V.S.A. § 2430(3), because they handle, collect, disseminate, or otherwise deal with nonpublic personal information of Vermont residents as defined by 9 V.S.A. § 2430(5), and are thus subject to the security breach notice requirements of Vermont law, 9 V.S.A. § 2435.
12. Defendants are and at all times relevant hereto have been "persons" under Vermont law, 1 V.S.A. § 128, who are subject to the Consumer Fraud Act, 9 V.S.A. §§ 2451-2466.

Facts

13. On or about May 14, 2009, Defendant HNNE learned that a portable computer hard drive had disappeared from its Shelton Connecticut office.

14. Prior to May 14, 2009, the hard drive had been shipped from Defendant HNNE's Shelton, Connecticut office to Rancho Cordova, California for copying onto Defendant HN's servers in Rancho Cordova. When the planned data transfer could not be completed, the hard drive with all of its original contents was shipped back to Shelton, Connecticut. The drive was discovered missing after its return to Connecticut.

15. Defendant HNNE did not create a log file of the collection and transfer of the data included on the hard drive and as a result, could not readily determine the hard drive's contents when it went missing.

16. The information contained on the hard drive was not protected by encryption as that term is defined under HIPAA, 45 C.F.R. § 164.304, during either the trip to or from California.

17. The hard drive contained approximately 27.7 million scanned pages of documents related to the medical, personal, and financial information of approximately 1.5 million members of HN's health plan subsidiaries.

18. Included in the contents of the hard drive was the protected health information ("PHI" as that term is defined under HIPAA, 45 C.F.R. § 160.103), and personal information ("PI" as that term is defined under Vermont law, 9 V.S.A. § 2430(5)) of approximately 525 Vermont residents.

19 Defendants did not report the missing hard drive to the Connecticut police.

20. Defendants did not begin mailing notice letters to Vermont residents whose PHI and PI was, or was reasonably believed to have been, contained on the hard drive until

November 30, 2009 – more than six months after Defendants discovered the hard drive was missing.

21. No law enforcement agency requested that the consumer notice letters be delayed.

22. Defendants' November 30, 2009 letter to affected Vermont residents, attached as Exhibit A, stated in part:

> The purpose of this letter is to inform you of a matter involving an unencrypted portable computer disk drive that was discovered missing from a Health Net office. The information on the disk drive is in the form of scanned images rather than raw data and covers the period from 2002 to mid-2009. Because of the nature of the files saved on this portable computer disk drive, we were initially unable to determine what information was on the disk drive. The investigation to make this determination was very lengthy and required a detailed forensic review by computer experts. However, we have now been able to determine that the disk drive contained your personal information such as your name, address, Social Security number and possibly your protected health and financial information.
>
> Fortunately, the files on the missing drive were not saved in a format that can be easily accessible and therefore, we believe the risk of harm to you is low

23. The data contained on the hard drive was saved in TIF ("Tagged Image File") format with proprietary file extensions created by Defendants' document management system and was viewable through the use of freely available image-viewing software.

24. Defendants have at all times relevant hereto represented via their websites and other media that they have "adopted a strict guideline regarding the confidentiality" of protected personal information.

Count I: Violation of the Health Insurance Portability and Accountability Act (HIPAA)

25. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

26. HIPAA sets forth minimum standards governing the security of PHI that is transmitted by electronic media and maintained in electronic media as those terms are defined in 45 C.F.R. § 160.103. *See* 42 U.S.C. § 1320d-7; 45 C.F.R. § 160.203(b).

27 HIPAA requires covered entities to, *inter alia*:

a. ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information; protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information; and ensure compliance with HIPAA's security standards by the covered entity's workforce, 45 C.F.R. § 164.306(a)(1)-(4),
b. implement policies and procedures to prevent, detect, contain, and correct security violations; and identify and respond to a suspected or known security incident and mitigate, to the extent practicable, harmful effects that are known to the covered entity, 45 C.F.R. § 164.308(a)(1) & (6),
c. implement policies and procedures to limit physical access to electronic information systems; implement policies and procedures for all workstations that access electronic protected health information to restrict access to authorized users; and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility, to maintain their security, 45 C.F.R. § 164.310(a), (c) & (d),
d. implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights; and implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information, 45 C.F.R. § 164.312(a) & (b),
e. prevent improper use and disclosure of protected health information; and make reasonable efforts to limit protected health information to the minimum necessary to accomplish the covered entity's intended use, 45 C.F.R. § 164.502(a) & (b),
f. effectively train all members of the covered entity's workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their functions, 45 C.F.R. § 164.530(b) & 45 C.F.R. § 164.308(a)(5),
g. have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information, 45 C.F.R. § 164.530(c).

28. Defendants' conduct described above violates HIPAA and its implementing regulations.

Count II: Violation of Vermont's Security Breach Notice Act

29. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

30. The Security Breach Notice Act requires that data collectors notify affected individuals of security breaches "in the most expedient time possible and without unreasonable delay" 9 V.S.A. § 2435(b)(1).

31. Defendants' conduct described above violates the Security Breach Notice Act.

Count III: Violation of Vermont's Consumer Fraud Act

32. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

33. The Consumer Fraud Act prohibits unfair or deceptive acts or practices in commerce, 9 V.S.A. § 2453.

34. Defendants engaged in unfair or deceptive acts or practices contrary to Vermont's Consumer Fraud Act by failing to adhere to minimum standards of data security regarding the control, transfer, logging, and encryption of protected personal information, and by misrepresenting the risk of harm posed to Vermont residents by the disappearance of the unencrypted hard drive in Defendants' security breach notice letters.

Request for Relief

35. Wherefore, Plaintiff requests judgment against Defendants for relief as follows:

a. To enjoin Defendants from further violations as provided under 42 U.S.C. § 1320d-5(d)(l)(A);

b. To enjoin Defendants from further violations of 9 V.S.A. § 2435,

c. To enjoin Defendants from further violations of 9 V.S.A. § 2453;

d. Statutory damages as provided under 42 U.S.C. § 1320d-5(d)(2);

e. Civil penalties as provided under 9 V.S.A. § 2435(g);

f. Civil penalties as provided under 9 V.S.A. § 2458(b);

g. Awarding Plaintiff costs of this action and reasonable attorneys fees as provided under 42 U.S.C. §1320d-5(d)(3), 9 V.S.A. § 2435(g), 9 V.S.A. § 2458(b)(3).

36. Plaintiff asserts its right to a trial by jury on all issues so triable.

Dated: 1/14/11

Respectfully submitted,

WILLIAM H. SORRELL
ATTORNEY GENERAL
STATE OF VERMONT

Sarah E.B. London
Assistant Attorney General
Public Protection Division
109 State Street
Montpelier, Vermont 05609
802-828-5479
slondon@atg.state.vt.us

Counsel for State of Vermont

DEBIX
The Identity Protection Network

Register for Free Identity Protection

Health Net

Activation Code: <<code>>
Enroll Online. www.debix.com/healthnet
Assistance Hotline: 877-263-8001

<<FirstName>> <<LastName>>
<<AddressLine1>>
<<AddressLine2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>>

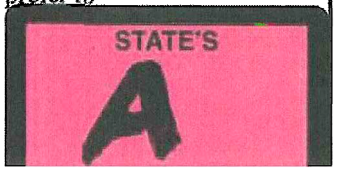
Dear <<FirstName>> <<LastName>>,

Protecting the privacy of our members' personal information is a critical priority at Health Net, Inc. The purpose of this letter is to inform you of a matter involving an unencrypted portable computer disk drive that was discovered missing from a Health Net office. The information on the disk drive is in the form of scanned images rather than raw data and covers the period from 2002 to mid-2009 Because of the nature of the files saved on this portable computer disk drive, we were initially unable to determine what information was on the disk drive. The investigation to make this determination was very lengthy and required a detailed forensic review by computer experts. However, we have now been able to determine that the disk drive contained your personal information such as your name, address, Social Security number and possibly your protected health and financial information.

Fortunately, the files on the missing drive were not saved in a format that can be easily accessible and therefore, we believe the risk of harm to you is low. Additionally, to date, the investigation has not found any evidence that any of the data contained on the disk drive has been misused. Nevertheless, we want to make you aware of the incident and the steps we are taking on your behalf to ensure you are as protected as possible.

To ensure the integrity of your personal information, Health Net has arranged for you to receive identity protection under the Debix Identity Protection Network, available for two years at no cost to you. Once you register, Debix will enroll you in their OnCall Credit Monitoring, and you will receive OnCall Credit Alerts regarding changes to your credit file. If the individual who has received this letter is under the age of eighteen, Health Net has arranged for them to receive credit protection services with Debix ChildScan. Using your phone, you can review and verify these Credit Alerts and the Debix OnCall Investigators are available to assist you in the event that you suspect any fraud relating to your personal accounts. The identity protection services also include $1,000,000 of identity theft insurance coverage and enrollment in Debix Fraud Resolution Services for two years, if needed, to assist you in restoring your credit file. Additionally, if you experienced any identity theft between May 14, 2009 and the date of this letter, Health Net has also arranged for Debix Fraud Resolution Services to restore your identity at no cost to you.

Debix has a simple internet-based verification and enrollment process. To enroll, visit www.debix.com/healthnet. You will need to provide the activation code listed at the top of this page. Once you have entered your activation code, click on "Sign Up Now" on the right side of the page and follow the website's instructions. Please note, if you enroll online, part of the enrollment process may include receiving a phone call from Debix soon after you initiate the registration process. If you prefer to register through the mail, please complete the enclosed mail-in registration form.



Should you choose not to enroll for the free Debix Identity Protection service, you should continue to check your credit report periodically to ensure fraudulent activity has not occurred. Even if you do not find any signs of fraud on your reports, we recommend that you remain vigilant and check your credit report every three months for the next year.

You may also want to contact the three credit bureaus included in the "State Specific Notification Requirements" attachment to discuss placing a fraud alert on your credit report. The credit bureaus are Equifax, Experian and TransUnion. Additionally, Health Net has arranged for you to be reimbursed for any fees associated with applying or thawing a credit freeze for a two year period. To learn more, please contact Debix at (877) 263-8001

We also recommend that you regularly review the explanation of benefit statements you receive from Health Net as claims are submitted. If you see any service that you believe you did not receive, please contact Health Net at the number on the statement. You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your one free credit report per year by calling (877) 322-8228 or visit www.annualcreditreport.com.

Health Net is diligent about ensuring the safety of our members' information. We are vigorously monitoring this matter to ensure the ongoing security of your private information and have implemented additional information security procedures. We sincerely regret any inconvenience or concern this event may cause you. In the meantime, we urge you to take advantage of the services available to you.

If you are interested in receiving identity protection services under the Debix Identity Protection Network, you must enroll in this service within 120 days from the date of this letter and the service will be valid for two years from your enrollment date. If you have any questions or feel that you have an identity theft issue, please contact our representatives at (877) 263-8001 between 9:00 a.m. and 5 00 p.m., CST, Monday through Saturday. You may also find answers to your questions online at www.debix.com/healthnet.

Sincerely,

Lisa King

Lisa King
Director, Information Privacy
Health Net, Inc.