VERMONT AG SETTLES DATA BREACH ENFORCEMENT ACTION FOR $55,000

BY MARC J. LEDERER

On January 21, 2011, the Vermont Attorney General settled an enforcement action against Health Net, Inc. and Health Net of the Northeast, Inc. (together, "Health Net") for the sum of $55,000. Arising out of a data breach involving the personal, financial and medical information of 525 Vermont residents, the enforcement action alleged violations of Vermont's Security Breach Notice Act, the Health Insurance Portability and Accountability Act ("HIPAA"), and Vermont's Consumer Fraud Act.

Facts of Data Breach

On May 19, 2009, Health Net learned that a portable computer hard drive was missing from the desk of an employee located in its Connecticut office. The missing hard drive contained the personal, financial and medical information of approximately 1.5 million persons, 525 of whom were Vermont residents. Contrary to company policy, the missing hard drive was unencrypted. Health Net began mailing letters giving notice of this breach to affected Vermont residents a little more than six months after the incident occurred, although not all of the letters were received by Vermont residents until more than a year after the hard drive went missing. Health Net claimed that they were unable to identify all of the affected individuals until about six months after the incident occurred.

Vermont's Enforcement Action

The enforcement action alleged violations of three sets of laws, namely, the Vermont Security Breach Notice Act, HIPAA, and the Vermont Consumer Fraud Act.

This is the first time an enforcement action has been brought under the Vermont Security Breach Notification Act, 9 V.S.A. § 2435, which requires that data collectors notify affected individuals of data breaches involving their personal information "in the most expedient time possible and without unreasonable delay." The Vermont Attorney General alleged that Health Net did not comply with this requirement because it began mailing out letters more than six months after the incident occurred.

Additionally, the Attorney General alleged that Health Net did not comply with sections of the federally enacted HIPAA, 45 CFR Parts 160 and 164, which require, among other things, that covered entities, such as those who provide health insurance plans, effectively secure an individual's protected health information.

Vermont's Consumer Fraud Act, 9 V.S.A. § 2453, prohibits unfair deceptive acts and practices in commerce. The Attorney General alleged that Health Net violated this law by failing to adhere to minimum standards of data security regarding the control, transfer, logging and encryption of protected health information, and by misrepresenting the risk of harm posed to Vermont's residents in its notification letters.

Mitigating Factors and Remedial Actions

The consent decree noted that Health Net represented that it concluded that there was a low risk of harm posed to Vermont residents because:

- the data on the missing hard drive was randomly saved and not searchable;
- information pertaining to Vermont residents represented only a small percentage of the overall data contained in the missing hard drive;
- it took Health Net approximately six months to identify a majority of the members referenced on the missing hard drive; and
- no known identity theft has occurred.

The consent decree also noted that Health Net represented that it has spent in excess of $7 million to remedy this data breach and that it has taken and/or will continue to take the following steps subsequent to the date of the incident:

- providing credit monitoring services, credit restoration services, and up to $1 million in personal internet identity insurance to all affected individuals;
- encrypting all external hard drives and other portable media used to transfer personal information or protected health information;
- encrypting all desktop computers and hard drives of company laptops;
- implementing technology that automatically logs all transfers and actual or attempted access of personal information or protected health information;
- implementing a combination of hardware and software that resides between the email server and the email client that is designed to identify email or attachments containing personal information or protected health information and automatically encrypt email containing such identified information before transmission.

Settlement Agreement Provisions

As a result of the agreed-upon settlement with Vermont, Health Net agreed to:

- pay the state of Vermont the amount of $55,000;

- retain a third-party data security auditor to evaluate the extent to which Health Net's information security programs and practices ensure the security, confidentiality and integrity of personal information and protected health information against future security breaches; and

- provide the Attorney General a written report that describes the auditor's assessment of Health Net's information security programs, describes the auditor's conclusions, identifies any of the auditor's recommended steps to improve Health Net's information security programs and practices, and identifies Health Net's plan for implementing the auditor's recommended steps. The initial report was to be provided by January 31, 2011, with a follow-up report to be submitted by January 31, 2013.

Conclusion

It should be noted that Health Net's breach not only resulted in the settlement with the Vermont Attorney General, but it resulted in similar earlier settlements with the Connecticut Attorney General in the amount of $250,000, the Connecticut Insurance Commissioner in the amount of $375,000, and with New York State. These settlements should serve notice to companies that states are actively enforcing their privacy and data breach laws. Accordingly, companies that collect or possess personal information or protected health information would well be advised to take preventive steps such as encryption of such data, and reactive steps to a data breach, such as responsibly expedient notification of affected persons, in order to minimize the damage to their resources and reputation.

About the Author: Marc J. Lederer is a Staff Attorney at Willkie Farr & Gallagher LLP (www.willkie.com). He can be reached via e-mail at mlederer@willkie.com or by phone at 212-728-8624.