FAEGRE & BENSON LLP

UNITED STATES | ENGLAND | GERMANY | CHINA

CRAIG KOMANECKI
CKomanecki@faegre.com
(612) 766-8982

March 25, 2009

VIA U.S. MAIL

Office of Attorney General Kelly A. Ayotte
33 Capitol Street
Concord, NH 03301

Re: Report of Data Security Breach

Dear Ms. Ayotte:

We represent Xcel Energy, a provider of energy products and services, headquartered in Minneapolis, Minnesota. As required by New Hampshire Statute § 359-C:19, I am writing to notify you of a data security breach that may have compromised the personal information of approximately 4 New Hampshire residents.

Xcel Energy has determined that, approximately two weeks ago, a member of its team responsible for processing employee access to Xcel Energy facilities sent an e-mail and spreadsheet attachment to another team member. The spreadsheet contained the name and Social Security number of a number of employees, including approximately 4 New Hampshire residents. The recipient of this e-mail then forwarded the same e-mail and attachment to other Xcel Energy managers as part of an employee training status update. Although all of these managers needed some of this information to perform their responsibilities, not all of the managers needed access to employee Social Security numbers.

The individual who made the initial mistake reported it immediately to Xcel Energy's information technology security team. We believe that all of the e-mails containing the spreadsheet were either successfully recalled or deleted from the system. We also believe, based on scans and other tests conducted by Xcel Energy's IT security team, that none of the e-mails were forwarded to non-employees and none were forwarded outside Xcel Energy's computer network. We have notified affected individuals by written notice.

Please find enclosed a copy of the written notification that has been sent to all Xcel Energy employees whose personal information may have been compromised.

If you have any questions regarding this matter, please contact me.

Very truly yours,

FAEGRE & BENSON LLP

Craig Komanecki

Enclosures
lb us.3803649 01

Xcel Energy®

414 Nicollet Mall
Minneapolis, Minnesota 55401-1993

March 23, 2009

<First Name> < Last Name>
<Street Address>
<City>,<State> <ZIP>

Dear <Title><Last Name>:

You either recently processed for access, or you currently maintain access, to work at our Monticello, Minnesota, nuclear generating plant. I am writing to inform you of a security incident that involves some personal information you provided in support of your request for access at Monticello. We are confident that there is little likelihood that your personal information will be misused as a result of this incident. However, because identity theft is a serious issue, we want you to know what happened so that you can take whatever steps you feel are appropriate to protect your information from any potential misuse.

Approximately two weeks ago, a member of our outage worker processing team at Monticello sent an e-mail with an attached spreadsheet to another team member. The spreadsheet contained some of your personal information, specifically your name and Social Security number. The recipient then forwarded the same e-mail and attachment to other Xcel Energy managers as part of a training status update. Normally the forwarding of this e-mail and attachment would have been an appropriate step in the process. However, the inclusion of Social Security numbers was a simple mistake and done in error. Although all of these managers are involved in overseeing training for their employees and contractors, not all of the managers needed access to your Social Security number to perform their responsibilities.

The individual who made the inadvertent error reported it promptly to our information technology (IT) security team. We believe that all of the e-mails containing the spreadsheet with your personal information were successfully recalled or deleted from our systems. We also believe, based on scans and other tests conducted by our IT security team, that none of the e-mails were forwarded to non-employees and none were forwarded outside Xcel Energy's computer network. Accordingly, there is little likelihood that your personal information will be misused as a result of this incident.

We are providing the enclosed information on the steps you can take to protect yourself from identity theft. In addition, we will reimburse you for the costs you incur in 2009 to run one credit report, to place a security freeze on your credit reports or to later remove that security freeze. You can receive reimbursement by sending us a copy of your receipt to the address listed below.

If you bave any questions regarding this incident, you can call us toll-free at 1-800-689-7662 during the hours of 9:00 a.m. to 5:00 p.m. C.D.T., Monday through Friday. You may also contact us in writing at 414 Nicollet Mall, Minneapolis, Minnesota, 55401, attention Access Manager.

CREDIT REPORT PROTECTION
FACT SHEET

Here are steps you can take to protect yourself from identity theft:

1. Place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening any new accounts or making any changes to your existing accounts. To place a fraud alert on your credit file, call any one of the three major credit bureaus listed below. Once one credit bureau confirms your fraud alert, the others will be notified to place fraud alerts on your credit file automatically. All three credit reports will be sent to you free of charge for your review. The three bureaus are:

Equifax	Experian	TransUnionCorp
P.O. Box 740241	P.O. Box 2104	P.O. Box 105281
Atlanta, GA 30374	Allen, TX 75013	Atlanta, GA 30348-5281
800-525-6285	888-397-3742	800-680-7289

2. When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Also look for personal information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. If you believe you are the victim of identity theft, contact your local law enforcement office or your state's Attorney General's office. Even if you do not find any suspicious activity on your initial credit reports, experts recommend that you monitor your account statements carefully and obtain and review your credit reports every three months for at least a year.

MASSACHUSETTS RESIDENTS

Under Massachusetts's law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts's law also allows you to place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from an individual's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been the victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies, Equifax, Experian and TransUnion, by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-679(
www.equifax.com	www.experian.com	www.transunion.com

In order to request a security freeze, you will need to provide the following information: full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five years; proof of current address such as a current utility bill or telephone bill; a legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.). If you are a victim of identity theft, include a copy of the police report, investigative report or complaint to a law enforcement agency concerning identity theft. If you are not a victim of identity theft, include payment by check, money order or credit card. Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

CALIFORNIA RESIDENTS

You may obtain information about avoiding identity theft from the California Office of Privacy Protection's Web site at www.privacy.ca.gov.

FOR ALL OTHER STATE RESIDENTS

You may obtain information about avoiding identity theft from the Federal Trade Commission's identity theft Web site at www.ftc.gov/microsites/edu/idtheft or by calling 1-877-IDTHEFT (438-4338).