CONFIDENTIAL

NEW HAMPSHIRE SECURITY BREACH REPORTING FORM

March 3, 2014

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Submitted by: EMC Corporation

Dear Attorney General Foster:

Pursuant to New Hampshire Rev. Stat. Ann. §359-C:20(I)(b), we are writing to notify you of a breach of security involving four New Hampshire residents.

Was this a breach at EMC? [X] No [ ] Yes
Was this a breach at an EMC vendor? [ ] No [X] Yes

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Date of the incident: Between 1/7/2014 and 1/30/2014

Nature of the incident (please select all that apply):
[ ] Hacking incident; [X] Inadvertent disclosure; [ ] Stolen computer, CD, tape, etc;
[ ] Lost computer, CD, tape, etc; [ ] Insider wrongdoing;
[ ] Other (specify):_____

An EMC vendor mistakenly sent an excel file containing personal information of EMC employees, including 4 employees who are residents of the State of New Hampshire, to unauthorized parties. The vendor did not realize that the personal information of EMC employees was contained in the excel file in question because there were filters on the file that had "hidden" the personal information. Upon learning of the security incident, the vendor notified EMC. The personal information contained in the excel file included the employees' (1) name; (2) employer name (EMC); (3) Social Security number; and (4) new and old addresses (street/city/state/zip).

Information Acquired (please select all that apply):
[X] Name; [X] SSN; [ ] Driver's license no.; [ ] Financial account number;
[ ] Credit or Debit card number; [X] Other (specify): address of employee

The information was in [X] electronic form and/or [ ] paper form.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Number of NH residents affected: 4

These NH residents have been sent written notice (copy included).

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

The security incident was inadvertently caused by an employee at an EMC vendor. The vendor confirmed in writing that all of the unauthorized recipients of the personal information have deleted the file in question. Additionally, the vendor has confirmed with EMC that the following measures have been taken to prevent repeat incidents: (1) additional training has been provided to staff members on the procedure for dissemination of any file containing personal information; and (2) the vendor is undertaking a formal review of the delivery method of files sent electronically.

Was the incident reported to law enforcement? [X] No [ ] Yes

- If Yes, which law enforcement entity?
    - Contact address of law enforcement entity, if available:

- If No, why not? The security incident was not the result of illegal activity. The unauthorized persons who accessed or may have accessed the file in question are working professionals who unintentionally received the unauthorized information.

CONTACT INFORMATION

If you have any questions, please contact Demetrios Eleftheriou in our Office of the General Counsel at 508-293-6327 or demetrios.eleftheriou@emc.com. Thank you.

EMC²

March 3, 2014

Name
Address
City, State Zip Code

Dear [Name],

We are writing to inform you that an EMC vendor that handles your Data General Retirement Plan experienced a security breach involving your personal information. The breach occurred between January 7, 2014 and January 30, 2014. The affected data includes your name, address and Social Security number.

We have already taken steps to address this incident and to protect your personal information from further unauthorized disclosure. In addition, we are enclosing a tip sheet that contains information about how to obtain copies of your credit reports (including free of charge), which you should review for any unexplained activity, and information about how to set up fraud alerts or security freezes on your accounts (fees may apply). A fraud alert lasts for 90 days. You can simply call one of the three credit reporting agencies at the number in the attached tip sheet. A security freeze prohibits a credit reporting agency from releasing any information from your 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.

We have retained InfoArmor, a specialist in identity theft protection, to provide you with 1 year of *"identity theft protection"* free of charge. You can enroll in the program by calling InfoArmor at 800-789-2720, Monday – Friday 7am to 5pm est. Please keep this letter; you will need the following personal access code in order to register for these services. Your personal access code is:

.

We encourage you to remain vigilant over the next 12 to 24 months and regularly review your bank and other financial account statements, as well as your credit report. If you notice any suspicious activity on any of your accounts or suspect identity theft, notify the relevant institution immediately, as well as the Federal Trade Commission and law enforcement as explained in the attached tip sheet.

For residents in North Carolina, you may also contact the North Carolina Attorney General's Office by phone at (919) 716-6400, on the Internet at http://www.ncdoj.com/, or by postal mail at 9001 Mail Service Center, Raleigh, NC 27699-9001.

Should you have any questions, please contact us at 508-249-2177

Sincerely,

Courtney Brown
Senior Director Global Compensation
EMC Corporation

EMC²

TIP SHEET OF HELPFUL INFORMATION

REVIEW YOUR CREDIT REPORTS

To obtain an annual free copy of your credit reports, visit www.annualcreditreport.com or call 1-877-FACT ACT. You may also contact the major credit reporting agencies directly:

- Equifax: 1-800-685-1111; P.O. Box 740241, Atlanta, GA 30374; www.equifax.com
- Experian: 1-888-397-3742; 475 Anton Blvd. Costa Mesa, CA 92626; www.experian.com
- TransUnion: 1-800-888-4213; 2 Baldwin Place, P.O. Box 2000, Chester, PA 19022; www.transunion.com

Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, or debts you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name, and employer(s). If any information is incorrect or you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

CONSIDER A FRAUD ALERT AND/OR SECURITY FREEZE

Consider contacting the fraud department of the three major credit reporting agencies to request that a "fraud alert" and/or "security freeze" be placed on your file, and include a statement that creditors must get your permission before any new accounts are opened in your name.

- Equifax: Fraud Alert: 1-800-525-6285 or http://www.equifax.com/answers/set-fraud-alerts/en_cp; Security Freeze: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian: Fraud Alert: 1-888-397-3742 or https://www.experian.com/consumer/cac/FCRegistration.do?alertType=INITIAL_ALERT; Security Freeze: 1-888-397-3742 or https://www.experian.com/consumer/cac/InvalidateSession.do?code=FREEZECENTER
- TransUnion: Fraud Alert: 1-800-680-7289 or e-mail to fvad@transunion.com; Security Freeze: 1-888-909-8872 or www.transunion.com/securityfreeze

SUGGESTIONS IF YOU SUSPECT YOU ARE A VICTIM OF IDENTITY THEFT

- **Obtaining and filing a U.S. police report**. Get a copy of the report from your local police department or sheriff's office. This may be necessary to submit to your creditors and others that may require proof of a crime in order to clear up your records.
- **Contact the U.S. Federal Trade Commission ("FTC")**. The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580; or online at www.consumer.gov/idtheft. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft."
- **Keep a record of your contacts**. Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.