6600 Stevenson Blvd.
Fremont, CA 94538
510-360-2222, Fax: 510-445-2020
www.oncorems.com

July 12, 2013

Dear Employee or Former Employee of OnCore Manufacturing:

We are writing to notify you of an incident that may affect the security of your personal information. While we are unaware of any attempted or actual misuse of your personal information, we are providing this notice so you are aware of the incident and you may take steps to monitor your identity and credit accounts should you decide to do so.

On July 5, 2013, a Company laptop of an Oncore employee was stolen from the employee's home along with all other valuable contents in their home. At the time of the theft, the laptop stored files including Oncore payroll reports for the following site locations and time period:
Fremont: 2013,
Longmont: 2007-current,
San Jose: 2007-current,
San Marcos: 2007-current,
Springfield: June 2012-current,
Wilmington: June 2012-current,
All other States or sites: June 2012 through current.

These reports included your name and Social Security Number, address, date of birth as well as other information relating to your employment. The laptop also contained reports on 401(k) remittances.

Oncore takes the theft and the security of your personal information very seriously. The theft was immediately reported to local law enforcement, whose investigation into this incident is ongoing. The laptop has not been recovered. Our notification to you was not delayed as a result of the police investigation. OnCore has employed certain security measures to track and automatically delete data from the stolen laptop. Oncore has also retained an independent third-party security expert to assist with the response to the theft.

We take the matter of ensuring the security of your personal information very seriously and have made arrangements with Experian for you to receive free credit monitoring for up to twelve months. At no cost to you, you are eligible to enroll in credit monitoring and support services.

You can activate credit monitoring and support services by following the instructions on the attached sheet. We urge you to sign up for the service as soon as possible in order to receive the greatest protection.

Oncore is unaware of any actual or attempted misuse of your personal information. Nevertheless, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. At no charge, you can also have these credit bureaus place a "fraud alert" or "security freeze" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note that because such an alert instructs creditors to follow certain procedures, it may also delay, interfere with or or prevent the timely ability to obtain credit, including new loans, credit mortgages, employment, housing or other services while the agency verifies your identity. Should you desire to place a fraud alert or obtain a credit report, please contact any one of the agencies listed below. As soon as one credit bureau confirms your fraud alert, the others will be notified to place fraud alerts on your file.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3724	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Here are some recommended steps that you may wish to undertake:

- ✓ Obtain a recent credit report (as described above) and perform an annual review to ensure that no unauthorized transactions have occurred.
- ✓ Place a 90-day fraud alert on your file (described above).
- ✓ Frequently monitor your credit cards for unauthorized transactions.
- ✓ Avoid using debit cards for Internet transactions and other purchases (e.g. gas station payments) since these types of transactions typically cannot be disputed with your financial institution.
- ✓ Avoid responding to any emails that appear to be coming from a financial institution. If necessary, call your financial institution directly to verify authenticity of the communication.
- ✓ Watch out for "phishing" emails asking for additional personal information or IDs based on incomplete information presented to you. Do not click on any Internet links or websites within these emails, especially when they appear suspicious.
- ✓ If you receive a phone call requesting personal information, do not provide any information over the phone to the caller. Ask for a callback number and corresponding company name from the caller. Verify the company's number from personal statements or from the back of credit cards if relevant. Alternatively, find the main phone number for the company to verify if a valid company representative did call you prior to providing personal information.
- ✓ Many websites and Internet email providers have dual authentication methods for signing in (e.g. a password and security image). Make sure you use these new security measures to prevent unauthorized users from accessing your account remotely. These security measures will alert you via text messaging, email, or a phone call.

- ✓ Avoid accepting friend invitations on social networking sites from people you do not know.

- ✓ Set stricter privacy policies on personal interactions (e.g. posts, check-ins, tweets, likes, etc.) on each social networking site that you use to be viewed by people on your friends list only.

If you are a resident of Illinois or North Carolina:

We are required to provide you with the contact information of the Federal Trade Commission as a resource from which you can obtain information about preventing identity theft.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
www.ftc.gov

If you are a resident of North Carolina:

We are required to provide you with contact information to the North Carolina Attorney General's Office as an additional resource for information about preventing identity theft.

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6400
Telephone: 1-877-566-7226
http://www.ncdoj.gov/

If you are a resident of Massachusetts:

Please be advised that 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. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift of 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.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). 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.

We sincerely apologize for any inconvenience and concern this may have caused you.

I am available to be reached at 510-360-2222 should you have any questions or concerns.

Very truly yours,

Zareen Mohta

Zareen Mohta
Vice President, Human Resources