ThyssenKrupp Materials NA
OnlineMetals Division

OnlineMetals.com
POINT. CLICK. METAL.

ThyssenKrupp

May 2, 2013

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Breach Notification

Dear Attorney General Delaney:

ThyssenKrupp OnlineMetals, LLC was recently informed by the company that hosts the OnlineMetals website, www.onlinemetals.com, that an intruder gained unauthorized access to the website server between approximately February 5, 2013 and March 10, 2013 by exploiting a vulnerability in a vendor product. This may have comprised "personal information" (as defined in N.H. Rev. Stat. 359-C:19) of approximately six (6) New Hampshire residents who made purchases through the website, including their names, credit or debit card numbers, and card verification numbers of customers, and possibly also their mailing addresses, e-mail addresses, and phone numbers.

We have taken some immediate measures to respond to the incident while we continue our investigation, including working with the website hosting company to implement additional security measures. We plan to notify the New Hampshire residents by letter on **5/13/13.**

We are committed to maintaining and protecting the confidentiality of our customers' personal, private, and sensitive information. We regret that this situation has occurred, and we will be working to reduce the risks of a similar situation happening in the future.

If you have any questions, please feel free to contact Michael Bauer, Assistant General Counsel, ThyssenKrupp North America, Inc. at (312) 525-2743 or michael.j.bauer@thyssenkrupp.com.

Sincerely,

Shawn Lynam
President

OnlineMetals.com
A Division of ThyssenKrupp Materials NA, Inc.
1138 W Ewing St. Seattle, WA 98119
Telephone: (206) 285-8603 or (800) 704-2157 • Fax: (206) 285-7836
Internet: www.onlinemetals.com

ThyssenKrupp Materials NA
OnlineMetals Division

OnlineMetals.com
POINT. CLICK. METAL.

ThyssenKrupp

May 2, 2013

Date]

[Name]
[Address]
[City, State, Zip]

Dear Valued Customer,

We are writing to inform you that personal information collected through the ThyssenKrupp OnlineMetals, LLC website, www.onlinemetals.com, may have been compromised. We deeply regret that this incident occurred, and because you are potentially affected, we want to share with you what we know and urge you to take steps to protect your personal information.

We were informed by the website hosting company that an intruder gained unauthorized access to the website server between approximately February 5, 2013 and March 10, 2013 by exploiting a vulnerability in a vendor product. This may have comprised the names, credit or debit card numbers, and card verification numbers of customers who made purchases at the website, and possibly also their mailing addresses, e-mail addresses, and/or phone numbers.

We have taken some immediate measures to respond to the incident while we continue our investigation, including working with the website hosting company to implement additional security measures. We also recommend that you take steps to protect yourself from the possibility of identity theft. First, you should review your credit and debit card account statements, and immediately report any suspicious or unauthorized activity to your provider. Second, we recommend that you contact the three major credit reporting agencies ("CRAs") to place a fraud alert and/or security freeze on your credit file. We have attached to this letter contact information for the CRAs and additional information about fraud alerts and security freezes. Please read it carefully, as there are differences between a fraud alert and security freeze.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Under federal law, you are entitled to a free credit report once a year. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If a report shows accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as a home address, that is inaccurate, or other information you do not understand, contact one of the credit bureaus immediately. You may visit www.annualcreditreport.com, a website sponsored by the three CRAs, for more information on how to request your credit report.

OnlineMetals.com
A Division of ThyssenKrupp Materials NA, Inc.
1138 W Ewing St. Seattle, WA 98119
Telephone: (206) 285-8603 or (800) 704-2157 • Fax: (206) 285-7836
Internet: www.onlinemetals.com

ThyssenKrupp Company

If you find suspicious activity on your credit reports or have reason to believe your personal information is being misused, you should take two steps. First, call local law enforcement personnel and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. Second, file a complaint with the FTC at www.ftc.gov/idtheft or 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. For additional information, you can write to: FTC, Consumer Response Center, Room 130-B, 600 Pennsylvania Avenue, N.W. Washington, D.C., 20580.

OnlineMetals, LLC is committed to maintaining and protecting the confidentiality of our customers' personal information. We regret that this situation has occurred, and we will be working to reduce the risks of a similar situation happening in the future. We sincerely apologize for any inconvenience this situation may have caused. If you have any questions, please feel free to contact our customer service by e-mail at sales@onlinemetals.com or call toll-free at 1 (800) 704-2157 M-F, 8:00 am – 5:00 pm.

Sincerely,

Shawn Lynam
President

.../3

How to Request a Credit Fraud Alert and Security Freeze

It is important to monitor your credit and be aware of unusual or fraudulent activity on any of your accounts. Here is some information on how to request a fraud alert and ask for a credit freeze, along with contact information for the three major national credit reporting agencies ("CRAs"), Equifax, Experian and TransUnion. There are differences between how the CRAs handle fraud alerts and security freezes, so please read this carefully.

Fraud Alert

A fraud alert is a statement added to your credit report that alerts creditors of possible fraudulent activity within your report, and requests that they contact you prior to establishing any accounts in your name. To place a fraud alert on your credit file, you may call or write to any of the CRAs. As soon as one CRA confirms your fraud alert, the others will be notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	**Experian**	**TransUnion**
1-877-478-7625	1-888-397-3742	1-800-680-7289
P.O. Box 740256	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

Security Freeze

A security freeze restricts a CRA from releasing any information from your credit report without your prior written consent. Many state laws provide consumers with a right to request a security freeze, and the three CRAs voluntarily offer this service to all U.S. consumers. To place a security freeze on your credit report, you must send a written request (some states permit telephone requests) to one of the three major CRAs at the addresses identified below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, Georgia 30348	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

CRAs may charge a fee for implementing the security freeze (generally from $5 to $10) depending on the laws of the state in which you reside, but many state laws require the CRAs to waive the fee for victims of identity theft who submit a valid investigative or incident report or complaint filed with a law enforcement agency. Additional fees may apply for temporarily or permanently removing a security freeze. CRAs may also require you to submit a copy of a government issued identification

.../4

card and other documents as proof of your identity. However, note that the CRAs treat security freezes differently from fraud alerts.

To effectively freeze access to your credit files, you should request the security freeze at all three major CRAs, as the CRAs do not share security freeze information with each other. Each of the CRAs requires slightly different information, so you should contact each CRA to find out exactly what is required.