GRAFTech International

GrafTech International Holdings Inc.
12900 Snow Road • Parma, Ohio 44130

Melissa A. Dials
Attorney

VIA REGULAR MAIL

January 20, 2011

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

Subject: Personal Information Security Breach Notification

Dear Attorney General Delaney,

Pursuant to New Hampshire Statutes §359-C:20(I)(b), we are writing to notify you of a security breach involving the personal information of one (1) New Hampshire resident.

We have learned that a GrafTech company laptop computer was stolen on January 7, 2011. We believe personal information of some of GrafTech's current and former US employees may have been accessible on this laptop. However, there is no indication that this laptop was stolen with the intent to access this personal information or that any personal information has been misused or compromised as a result of this incident. A police report has been filed and we are working with the proper authorities.

On January 15, 2011, the enclosed communication was sent to all current U.S. employees for which GrafTech has an email address on file, or by delivery to the union representing employees for which GrafTech does not have an email address on file for subsequent delivery to such employees at the beginning of their next work shift. Additionally, on January 19, 2011, the enclosed letter and attachments were sent in hard copy to all current and former US based employees by First Class mail. The one (1) individual who is a New Hampshire resident was sent notification as described herein.

If you require additional information please do not hesitate to contact me at the address above.

Sincerely yours,

Melissa Ann Dials
Corporate Counsel

Enclosures

GRAFTech International

To: GrafTech US Team Members
Date: January 15, 2011
Subject: Data Security Incident Questions & Answers

What happened?
We have learned that a GrafTech laptop was stolen on January 7, 2011. We believe personal information of some of our U.S. based team members may have been accessible on this laptop. A police report was filed and we are working with the proper authorities.

How many people could be impacted and what type of personal information was possibly revealed?
We cannot determine with certainty those specifically affected, given that the laptop has not been recovered. We believe that varying levels of information may be accessible including full name, address, birth date, Social Security number and bank information.

However, there is no indication that the laptop was stolen with the intent to access this personal information, and there is no evidence that anyone's personal information has been compromised or misused as a result of this incident.

If this incident occurred on January 7, why are we just being informed now?
Although steps were taken immediately to secure the data, it required some time to investigate the incident. This was necessary to ensure we had a clearer understanding of the information involved. We apologize if it seems that this process took longer than desired, but please be assured the matter was of the highest priority and conducted as swiftly and accurately as possible.

What is GrafTech doing to address this incident?
We are engaging the services of a credit monitoring and identity theft resolution company to provide assistance to all US-based team members. You will receive an overview of its services and how to enroll next week. GrafTech will provide free credit monitoring for two years to help protect against fraudulent activity as it relates to your personal identity.

If I think I have been a victim of credit fraud, what should I do in the meantime?
The Federal Trade Commission has released a comprehensive guide that may provide you with valuable information to help protect yourself against and deal with identity theft. It is available for free online at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html or by calling 1-877-ID-THEFT.

For your convenience, the three major credit reporting agencies details are listed below, should you wish to contact them directly.

Equifax
Direct Line for reporting suspected fraud:
1-800-525-6285
Fraud Division
P.O. Box 105069
Atlanta, GA 30348
http://www.equifax.com/answers/set-fraud-alerts/en_cp

Experian
Direct Line for reporting suspected fraud:
1-888-397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
https://www.experian.com/fraud/center.html

TransUnion
Direct Line for reporting suspected fraud:
800-680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page

Who should I contact if I have any additional questions concerning this incident?
In order to answer any questions that you may have regarding this incident, the HR Benefits line is available at Please also feel free to contact your local HR representative with any questions.

I haven't found anything suspicious with my accounts. Is my identity safe?
While there may be an indication that things are fine, please continue monitoring your financial statements and your credit report. We strongly encourage you to sign up for the free service being provided to monitor your credit for the next two years.

What is GrafTech doing to make sure this doesn't happen again?
We are taking this opportunity to review our procedures for protecting data and to educate team members about ways to further protect their personal information. We will also continue our work to help prevent future incidents from occurring.

GRAFTech
GrafTech International Ltd

GrafTech International Holdings Inc.
12900 Snow Road • Parma, Ohio 44130

Brian E. Blowes
Vice President, Human Resources

January 19, 2011

Dear GrafTech Team Member:

Please read this letter in its entirety.

GrafTech takes its commitment to safeguarding the personal information and security of our team members very seriously.

This letter is to notify you that your personal information may have been compromised in a recent theft of GrafTech property. We also would like to update you on precautions that we are taking to help ensure that your information is fully protected and secure, as well as some steps that you may wish to take on your own.

We have learned that a GrafTech laptop containing team member information was stolen on January 7, 2011 in Monterrey, Mexico. We believe personal information of some of our U.S. based team members may be accessible on this payroll laptop. However, there is no indication that this laptop was stolen with the intent to access this personal information. A police report was filed and we are working with the proper authorities.

As a precaution, we ask that you monitor your financial accounts carefully for suspicious activity and take appropriate steps to protect yourself against potential identity theft. To assist you in this effort, GrafTech has partnered with **Identity Theft 911** to offer, at no cost to you, credit monitoring and identity theft resolution services for the next two years.

These services are available should you have any questions, think you may have a problem or in the unlikely event that you become an identity theft victim. Access to this service will last for two full years and will include the following:

- Unlimited access to services via a toll-free number or secure website
- Systematic notification to credit bureaus, creditors and collectors, government agencies, and relevant parties if necessary
- All phone calls and documentation needed to resolve your identity theft, should you become a victim
- Comprehensive case file creation to assist law enforcement, if necessary
- Credit report*
- Credit monitoring*
- Fraud, Identity Theft and Privacy education*
- One year of follow-up alerts, phone calls, and status checks to avoid recurrence

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age

Please note that when signing up for the credit monitoring products, you may be asked to verify personal information for your own protection and in order to confirm your identity.

We strongly recommend that you enroll in these free services by logging on to [redacted] or **calling the Identity Theft 911 help line at** [redacted] ***You will be asked to provide the following unique code to receive services:*** **XXXXXXXXXX**. You will have 12 months from the date of this letter to sign up for these services.

In addition, the US Federal Trade Commission has released a comprehensive guide that may provide you with valuable information to help protect yourself against and deal with identity theft. It is available for free online at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html or by calling 1-877-ID-THEFT.

Please be assured that we are carefully reviewing our systems access and security methods to help prevent this from recurring in the future.

Again, while we have no evidence that your personal information has been misused or compromised as a result of this incident, we believe it is important that you are fully informed of the potential risks and that you enroll in the above free credit monitoring and identity theft resolution services.

A list of anticipated questions and answers is attached for your reference. If you have any additional questions, please feel free to discuss with your local HR manager, or call the GrafTech HR shared service center at [redacted]

GrafTech sincerely regrets any inconvenience this situation may cause, and we will do our best to resolve any issues arising as a result of it.

Sincerely,

Brian Blowes

Attachment

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age

January 19, 2011

Dear GrafTech Team Members:

GrafTech takes its commitment to safeguarding the personal information and security of our team members very seriously.

We have learned that a GrafTech laptop containing U.S. based team member personal information was stolen on January 7, 2011. There is no indication that this laptop was stolen with the intent to access this personal information or misuse this information in any manner. A police report was filed, the affected personnel have already been contacted and we are working with the proper authorities to resolve the incident. While non-U.S. team members are not impacted by this situation, we are alerting you to this event to create additional awareness around laptop and cell phone security.

Please be assured that we are also carefully reviewing our systems access and security methods to help prevent this incident from recurring in the future.

We would like to take this opportunity to remind you of the importance of protecting your identity from fraud and theft. We also ask you to carefully protect all sensitive Company information and equipment, including laptops. For the complete laptop policy, please visit the IT Policies page on the intranet: [redacted]

Again, while we have no evidence that the personal information of any U.S. based team members has been misused or compromised as a result of this incident, we believe it is important that ALL GrafTech team members are fully informed of the incident.

GrafTech sincerely regrets any inconvenience this situation may cause, and are doing our best to resolve any issues arising as a result of it.

Sincerely,

Brian Blowes
Vice President of Human Resources

GRAFTech International

To: GrafTech US Team Members
Date: January 19, 2011 update to Notice of January 15, 2011
Subject: Data Security Incident Questions & Answers

What happened?
We have learned that a GrafTech laptop was stolen on January 7, 2011 in Monterrey, Mexico. We believe personal information of some of our U.S. based team members may have been accessible on this payroll laptop. A police report was filed and we are working with the proper authorities.

How many people could be impacted and what type of personal information was possibly revealed?
We cannot determine with certainty those specifically affected, given that the laptop has not been recovered. We believe that varying levels of information may be accessible including full name, address, birth date, salary, Social Security number and bank account number.

However, there is no indication that the laptop was stolen with the intent to access this personal information, and there is no evidence that anyone's personal information has been compromised or misused as a result of this incident.

If this incident occurred on January 7, why are we just being informed now?
Although steps were taken immediately to secure the data, it required some time to investigate the incident. This was necessary to ensure we had a clearer understanding of the information involved. We apologize if it seems that this process took longer than desired, but please be assured the matter was of the highest priority and conducted as swiftly and accurately as possible.

What is GrafTech doing to address this incident?
We are engaging the services of Identity Theft 911, a credit monitoring and identity theft resolution company, to provide assistance to all US-based team members. The attached letter includes an overview of their services and instructions on how to enroll. GrafTech is providing these services, at no charge to you, for a period of two years.

What can I do on my own to address this situation?
Identity Theft 911 has been retained to help you with any questions or problems you may encounter, including obtaining a credit report/credit monitoring and placing fraud alerts for you. However, if you choose not to use these services, you are strongly urged to remain vigilant by monitoring your banking and credit transactions, reviewing your credit card and bank account statements, and obtaining and monitoring your credit reports for potential unauthorized activity. We also advise you of some additional steps you can take:

1. You can place a security freeze on your credit file. A security freeze allows you to prevent anyone from gaining access to your credit file to obtain new credit without your express authorization. A security freeze is a preventative measure against a form of

identity theft. This is especially important when someone who has access to your personal information seeks to get new credit in your name. To place a security freeze on your credit file, you must contact each of the credit reporting agencies listed in this notice (i.e., Experian, TransUnion and Equifax) separately, and there may be a fee charged by each consumer reporting agency. GrafTech will reimburse any documented fees charged by the reporting agencies for this freeze. However, Identity Theft 911 may also be able to assist with a security freeze at no additional charge depending on your circumstances (see cover letter). We encourage you to contact Identity Theft 911 to discuss your situation and determine if a security freeze is warranted. A security freeze typically will remain in place until you take action to lift it either permanently or temporarily.

2. You can also contact any of the credit reporting agencies listed in this notice and ask that they put a fraud alert on your credit file. A fraud alert essentially notifies creditors to take additional steps to verify your identity prior to granting credit in your name. While a fraud alert will not prevent creditors from gaining access to your credit file, it may make it more difficult for someone to obtain credit in your name. Please note that because a fraud alert tells creditors to follow certain procedures, it also may delay your ability to obtain credit while the agency verifies your identity. There is typically no fee for a fraud alert. Fraud alerts may be temporary, lasting for a limited period of time. In that event, you would need to decide whether to renew the fraud alert when it expires. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any of the credit reporting agencies listed in this notice.

3. You are also entitled under U.S. law to one free credit report annually from each of the three major credit reporting agencies. As stated above, we advise you to obtain and monitor your credit reports for potential unauthorized activity. When you get your credit reports, examine them for any accounts that you did not authorize or any other entries that may indicate that your personal information has been misused or compromised. You should also carefully examine any credit card, bank account or other financial account statements for unauthorized charges or other unauthorized activity.

4. You may wish to contact your financial institution to provide notification that your bank or other financial account information may have been compromised and to ask them to put a password on your account so that access to your accounts, and inquiries, changes, or withdrawals, cannot be made without the password. Your passwords should be kept confidential, protected from unauthorized discovery or access, and not disclosed to others. Your financial institution may require or encourage you to create passwords with certain attributes and to change your passwords periodically.

5. The Federal Trade Commission (FTC) has released a comprehensive guide that may provide you with other valuable information to help protect yourself against and deal with identity theft. It is available for free by contacting the FTC directly:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

6. For your convenience, the three major credit reporting agencies details are listed below, should you wish to contact them directly.

Equifax
Direct Line for reporting suspected fraud:
1-800-525-6285
Fraud Division
P.O. Box 105069
Atlanta, GA 30348
http://www.equifax.com/answers/set-fraud-alerts/en_cp

Experian
Direct Line for reporting suspected fraud:
1-888-397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
https://www.experian.com/fraud/center.html

TransUnion
Direct Line for reporting suspected fraud:
800-680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page

Who should I contact if I have any additional questions concerning this incident?
In order to answer any questions that you may have regarding this incident, the HR Benefits line is available at [redacted] Please also feel free to contact your local HR representative with any questions.

I haven't found anything suspicious with my accounts. Is my identity safe?
While there may be an indication that things are fine, please continue monitoring your financial statements and your credit report. We strongly encourage you to sign up for the free service being provided to monitor your credit for the next two years.

What is GrafTech doing to make sure this doesn't happen again?
We are taking this opportunity to review our procedures for protecting data and to educate team members about ways to further protect their personal information. We will also continue our work to help prevent future incidents from occurring.