



Titanium Metals Corporation  
224 Valley Creek Blvd.  
Exton, PA 19341  
Matt O'Leary  
Vice President & Associate General Counsel  
e-mail: matthew.oleary@timet.com

August 13, 2009

Office of Attorney General Martha Coakley  
One Ashburton Place  
Boston, MA 02108

Dear Attorney General Coakley:

I am writing on behalf of Titanium Metals Corporation ("TIMET") to inform you of a security breach potentially affecting eight Massachusetts residents. TIMET has determined that malicious software circumvented the Company's firewall protections and downloaded information from the Company's systems. This information was not encrypted. TIMET's Information Services Department discovered and stopped the cyberattack.

TIMET promptly retained an outside firm with special expertise in computer forensics to examine the affected computer equipment and attempt to identify the files that were downloaded. After an extensive investigation, the computer forensic experts reported on July 30, 2009, that they could not eliminate the possibility that some of the downloaded data included employees' personal information, primarily Social Security numbers. We cannot confirm whether any employee's personal information was, in fact, downloaded. Nonetheless, in an abundance of caution, we are providing notice to you and the individuals whose personal information may have been compromised.

TIMET has worked diligently to determine the identity of the Company's employees whose personal information may have been compromised by this cyberattack. TIMET has been able to determine that, as noted above, eight employees who reside in Massachusetts may have been affected. TIMET will mail the formal notice of security breach today. A copy of the letter that will be sent to affected Massachusetts residents is attached. As the letter reflects, TIMET has offered one year of free credit monitoring with Experian to affected individuals.

If you have any questions concerning the matters discussed above, please do not hesitate to call me.

Very truly yours,

A handwritten signature in black ink, appearing to read "Matt O'Leary", is written over a horizontal line.

Matthew O'Leary  
Vice President and Associate General Counsel  
Titanium Metals Corporation



TITANIUM METALS CORPORATION  
THREE LINCOLN CENTRE  
5430 LBJ FREEWAY, SUITE 1700  
DALLAS, TEXAS 75240-2697



TELEPHONE: 972.233.1700  
TELEPHONE FACSIMILE: 972.448.1445

August 12, 2009

«First» «Last»  
«Address»  
«City», «State» «Zip»

TIMET recognizes the importance of safeguarding employees' personal information. To that end, the Company has implemented administrative, technical and physical safeguards for that information. Even the most rigorous safeguards, however, can not guarantee protection against criminal conduct.

TIMET recently was victimized by such conduct, and we regret that this crime might have a direct impact on you. More specifically, malicious software circumvented the Company's firewall protections and downloaded information from the Company's systems. Fortunately, our Information Services Department discovered and stopped this cyberattack.

TIMET promptly retained an outside firm with special expertise in computer forensics to examine the affected computer equipment and attempt to identify the files that were illegally downloaded. After an extensive investigation, the computer forensic experts reported on July 30, 2009, that they could not eliminate the possibility that some of the downloaded data included personal information, primarily social security numbers related to some of TIMET's current and former employees and retirees. We cannot confirm whether any employee personal information was, in fact, downloaded or whether any of the downloaded information has been misused. Nonetheless, we are in the process of reviewing our security procedures and will take additional steps, if necessary, to prevent a recurrence.

In addition, out of an abundance of caution, we have taken several steps to help protect you against the possibility that your personal information was included in the download data and might be misused. To begin with, we have arranged for **one year of credit monitoring through ConsumerInfo.com, Inc., an Experian® company, at no cost to you.** If you choose to enroll in the product membership, known as **TripleAlert<sup>SM</sup>**, you will enjoy the following benefits:

- Daily monitoring of your credit report at each of the three national credit bureaus;
- Notification of key changes that may help you to identify possible fraudulent activity;
- Monthly "no-hit" notifications if no key changes were detected on your credit reports;
- \$25,000 (\$10,000 for residents of New York) of identity theft insurance, provided by Virginia Surety Company, Inc.;
- If you are victimized by identity theft, a dedicated representative will provide you with fraud resolution services free of charge.

You have ninety (90) days from the date of this letter to activate this membership. You can enroll on-line at <http://partner.consumerinfo.com/timet> by entering the activation code provided below. You will be instructed on how to initiate your online membership. If you have

«First» «Last»  
August 12, 2009  
Page 2



any questions concerning TripleAlert, or prefer to enroll over the phone for delivery of your membership via US mail, please call **1-866-252-0121**.

Your Credit Monitoring Activation Code is «Code».

In addition to arranging for one year of free credit monitoring, we have prepared the **Recommended Steps** enclosed with this letter. The enclosure provides you with additional information on how to protect yourself against the possibility of identity theft. Please review it carefully.

TIMET recognizes that the possible theft of your personal information, and any related inconvenience, might cause you concern. We regret that this crime against TIMET may have put your personal information at risk and we will continue our efforts to prevent similar criminal activity in the future.

If you have any questions, please call 1-877-378-1286.

Sincerely,

A handwritten signature in black ink, appearing to read "Keith S. D'Souza". The signature is fluid and cursive, written in a professional style.

Keith S. D'Souza  
Vice President - Human Resources

### **Additional Information For Massachusetts Residents**

You have the right under Massachusetts law to report this incident to the police located in the county where you reside and to receive a police incident report from that police department within twenty-four hours of filing the report.

You have the right under Massachusetts law to place a "security freeze" on your credit report with the national credit bureaus. A security freeze prohibits the consumer reporting agency, with limited exceptions, from releasing any information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent.

You can request a security freeze by sending written notice to each of the national credit bureaus at the addresses listed below. Your request must include the following information about you: (a) full name, with middle initial and generation, such as JR, SR, II, III, *etc.*; (b) Social Security number; (c) date of birth (month, day and year); (d) current address and previous addresses for the past two years; and (e) the \$5 fee or a valid police incident report. You can pay by personal check or by credit card. For credit card payment, you will need to provide the following information: (a) name of the person as it appears on the credit card; (b) type of credit card (*e.g.*, American Express, Mastercard, VISA, or Discover Card); (c) complete account number; (d) expiration data (month and year); (d) for American Express - 4 digit Card Identification Number (on front of card above the account number); for Mastercard, VISA, or Discover Card - 3 digit Card Identification Number (on back of card at the end of the account number).

You also must include one copy of a government-issued identification card, such as a driver's license, state or military ID card, *etc.*, and one copy of a utility bill, bank or insurance statement, *etc.* Each copy must be legible (enlarge if necessary), display your name and current mailing address, and the date of the statement (statement dates must be recent).

## Recommended Steps

By immediately taking the following steps, you can help reduce the risk that your personal information will be misused.

**1. Activate the credit monitoring paid for by TIMET.** You must personally activate credit monitoring for it to be effective.

The Notification Letter included in this mailing will provide you with instructions and information to activate the TripleAlert credit membership. If you need assistance, you can contact Experian directly at **1-866-252-0121**. With Experian's credit monitoring, you will receive:

- Automatic, daily monitoring of the Experian, Equifax and TransUnion credit files;
- Notification within 24 hours of critical changes to your credit report. You will quickly find out about changes, including potentially fraudulent activity such as new inquiries, new accounts, late payments, and more;
- Monthly "no-hit" notices, letting you know there were no changes with your credit activity;
- Toll-free access to fraud resolution specialists who help investigate each incident; contact credit grantors to dispute charges, close accounts and compile documents; and contact all relevant government agencies and law enforcement officials as needed;
- \$25,000 of identity theft insurance with zero deductible provided by Virginia Surety Company, Inc. for certain identity theft expenses. (Insurance coverage is \$10,000 for residents of New York and is not available in US overseas commonwealths or territories (e.g., Puerto Rico)).

Enrolling in TripleAlert will not affect your credit score.

**2. Place a fraud alert with one of the three national credit bureaus.**

You can place a fraud alert with one of the three national credit bureaus by phone and also via Experian's website. If you elect to participate in the credit monitoring as discussed in #1, above, please wait until **after** you have activated the credit monitoring before placing a fraud alert. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
(800) 525-6285  
P.O. Box 740241  
Atlanta, GA 30374-0241

Experian Fraud Reporting  
(888) 397-3742  
P.O. Box 9532  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
(800) 680-7289  
Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790

You need to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place an alert on their records as well. You will receive confirmation letters in the mail and will then be able to order a credit report from each of the three credit bureaus, free of charge, for your review.

## Recommended Steps

Page 2

- 3. Review your credit reports.** You can receive free credit reports by placing a fraud alert and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.
- 4. Review your account statements.** You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers.
- 5. Respond to suspicious activity.** If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. If you receive an e-mail alert from Experian, contact an Experian fraud resolution representative at 1-866-252-0121. You also should consider notifying your local police department and the Federal Trade Commission of any suspicious activity involving your account statements or credit reports.
- 6. Additional Information.** You can obtain additional information about steps you can take to avoid identity theft from the following:

Identify Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>  
(877) IDTHEFT (438-4338)  
TDD: (202) 326-2502

