LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

September 9, 2022

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, New Hampshire 03301
Email: doj-cpb@doj.nh.gov

Re: Notification of Data Security Incident

To Whom it May Concern:

We represent TIC International Corporation ("TIC"), located in Carmel, Indiana, in connection with a recent data security incident described below. The purpose of this letter is to provide formal notice to your office.

I. Nature of Security Incident

On March 30, 2022, TIC experienced a system disruption due to an encryption attack. TIC engaged a digital forensics firm to assist with their response and to determine whether any personal information was affected. The investigation confirmed that personal information had been acquired without authorization. TIC then engaged an independent data review team to conduct an extensive review of potentially affected files to determine what personal information may have been involved, locate mailing information, and set up the services being offered to affected individuals. This process was completed on August 22, 2022.

II. Number of New Hampshire Residents Affected

Forty-two (42) residents of New Hampshire were affected by and notified of this incident. The affected information for these individuals includes a name in combination with a Social Security number.

A notification letter was sent to these individuals via first class U.S. mail on September 6, 2022. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

As soon as TIC became aware of the incident, it launched an investigation, engaged a digital forensics firm to assist with the investigation, and worked to determine whether any personal information was acquired without authorization. They also implemented measures to enhance the security of its network.

Once TIC determined which consumers were affected by this incident, it immediately began the process of locating addresses in order to notify them and provide information to consumer reporting agencies regarding the incident. As part of this notice, TIC is offering affected residents twelve (12) months of credit and identity monitoring, a $1,000,000 identity theft insurance reimbursement policy, and fully managed identity theft recovery services. They are also providing, through Kroll, a fully staffed call center to answer questions and provide support to affected individuals.

IV. Contact Information

If you have any questions or need additional information, please contact me at 971.712.2795 or sean.hoar@lewisbrisbois.com, or Jamie Seibert at 202.926.2907 or jamie.seibert@lewisbrisbois.com.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl. Sample Consumer Notification Letter

TIC International Corporation
Benefit Administrators and Consultants
11590 North Meridian Street, Suite 600
Carmel, Indiana 46032-4529

<<b2b_text_4(MICHINGAN STATE PAINTERS INSURANCE FUND)>>

<<b2b_text_5(PAINTERS LOCAL UNION NO. 1052 PENSION TRUST FUND)>>

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Re: Notice of Data Breach/ Data Incident)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to provide you with information about a recent data security incident that may have involved your personal information. TIC International Corporation ("TIC") administers health, pension, defined contribution/401(k), and other types of benefit funds. TIC is required to maintain records of your personal information because you are or have been a Participant of <<b2b_text_2 (Fund Names)>>. The purpose of this letter is to inform you about the incident, offer you identity monitoring services, and provide you with information, resources, and other steps you can take to help protect your personal information.

What Happened? On March 30, 2022, TIC experienced a system disruption due to an encryption attack. We hired cybersecurity experts to assist with our response and to determine whether any personal information was affected. The investigation determined that personal information was acquired during the incident. Following this confirmation, we underwent a thorough and extensive review of potentially affected files to determine what personal information may have been involved, locate mailing information, and set up the services being offered, which process was completed on August 22, 2022.

What Information Was Involved? The information involved included your <<b2b_text_3 ("name" and Data Elements)>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also reported the matter to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable. We have also secured the services of Kroll to offer identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of their confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. We encourage you to activate the free identity monitoring services.

For More Information: Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact <<Toll Free Number>>, Monday through Friday, 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Ronald T. Fisher
Corporate Privacy and Security Officer

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www riag ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.