

**BakerHostetler**

RECEIVED

FEB 23 2021

CONSUMER PROTECTION

**Baker & Hostetler LLP**

2929 Arch Street  
Cira Centre, 12th Floor  
Philadelphia, PA 19104-2891

T 215.568.3100  
F 215.568.3439  
www.bakerlaw.com

Benjamin D. Wanger  
direct dial: 215.564.1601  
bwanger@bakerlaw.com

February 22, 2021

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, ITOCHU International Inc. ("III"), to notify you of a security incident involving two New Hampshire residents.

III recently concluded an investigation of an incident that involved unauthorized access to one employee's email account. Upon first learning of the potential access to the employee's email account, III immediately secured the account and launched a thorough investigation. A third-party cybersecurity forensics firm was engaged to assist.

Through this investigation, completed on December 8, 2020, III discovered that an unauthorized party gained access to the employee's email account between September 8, 2020 and September 9, 2020. The investigation was unable to determine whether the unauthorized party actually viewed any emails or attachments in the account. In an abundance of caution, III reviewed the emails and attachments that may have been viewed in the email account to identify individuals whose personal information may have been accessible to the unauthorized party. The investigation was unable to rule out the possibility that the unauthorized party may have been able to access emails and/or attachments containing the names and Social Security numbers of two New Hampshire residents.

On February 22, 2021, in accordance with N.H. Rev. Stat. Ann. § 359-C:20, III is providing written notice via United States Postal Service mail to the two New Hampshire residents whose personal information was potentially accessed by an unauthorized party.<sup>1</sup> To help monitor for any potential misuse of personal information, III is offering a complimentary one-year membership in credit monitoring and identity theft protection services through Kroll to the affected New Hampshire

---

<sup>1</sup> This notice does not waive III's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

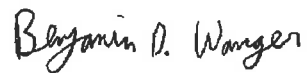
February 22, 2021

Page 2

residents. The notice letter also provides a telephone number that notice recipients can call with any questions they may have.

To help prevent a similar incident from occurring in the future, III has implemented additional security measures to enhance the security of its network and retrained all employees concerning data retention and security.

Please do not hesitate to contact me if you have any questions regarding this matter.

A handwritten signature in black ink that reads "Benjamin D. Wanger". The signature is written in a cursive style with a clear, legible font.

Benjamin D. Wanger  
Counsel



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<last\_name>>:

ITOCHU International Inc. (“III”) understands the importance of protecting the information we maintain. We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking.

III recently concluded an investigation of an incident that involved unauthorized access to one employee’s email account. Upon first learning of the potential access to the employee’s email account, we immediately secured the account and launched a thorough investigation. A third-party cybersecurity forensics firm was engaged to assist.

In connection with that investigation, we learned that an unauthorized party gained access to the employee’s email account between September 8, 2020 and September 9, 2020. Our investigation was unable to determine whether the unauthorized party actually viewed any emails or attachments in the account. In an abundance of caution, we reviewed the emails and attachments that may have been viewed in the email account to identify individuals whose personal information may have been accessible to the unauthorized party. On December 8, 2020, we determined that the account included an email and/or attachment containing your <<b2b\_text\_1(DataElements)>>

We believe that the unauthorized access occurred as part of an attempt to obtain money from III through a wire transfer and not to access personal information. While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident. We encourage you to remain vigilant by regularly reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. As a precaution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **May 13, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To help prevent a similar incident from occurring in the future, we have implemented additional security measures to enhance the security of our network and we are retraining our employees concerning data retention and security. If you have any questions about this incident, please call 1-855-763-1157 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,

Shiro Saito  
Director – Information Systems

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services<sup>1</sup> from Kroll:

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

### **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.

<sup>1</sup> 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.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

### Additional Information for Residents of the Following States

**North Carolina:** You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)