



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

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

**Subject:** <<b2b\_text\_2 ([Notice of Security Incident/Notice of Data Breach])>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

We are writing you today to let you know about a data security incident that may have involved your personal information. The privacy and security of your personal information is extremely important to Great Lakes Wholesale Group, IIT-JMK ("Great Lakes"). That is why we are writing to inform you of the incident, offering you complementary identity monitoring services, and providing steps you can take to help protect your information.

**What Happened?** On or around August 26, 2019, Great Lakes discovered suspicious activity in our email environment. In response we began an investigation and hired a digital forensic firm to assist us with determining the extent of the incident and whether any individuals' personal information may have been affected. Based on the results of the investigation, it was determined that an unknown individual may have had limited unauthorized access to some emails from July 8, 2019 until September 22, 2019.

As a result, Great Lakes conducted a thorough analysis to determine whether any personal information may have been affected by the incident, and to identify the specific individuals whose personal information may have been impacted. Unfortunately, we determined on April 17, 2020 that your information may have been affected. While we do not have any indication that your personal information has been misused, we are informing you of the incident and providing you with access to complimentary identity monitoring services from Kroll out of an abundance of caution.

**What Information Was Involved?** The incident may have impacted your <<b2b\_text\_1 (name [and/, ] [Impacted Data])>>.

If your financial account number and/or payment card information is listed as potentially impacted, please verify whether the information provided to Great Lakes was your company's or your personal financial/payment card information. If this information was related to your company, please notify appropriate individual(s) at your company.

**What Are We Doing?** As soon as Great Lakes discovered the incident, we began taking action in response, as described above. We have also taken measures to further enhance the security of personal information in our possession and to prevent similar incidents from happening in the future, including increased and changed access controls.

We are also providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering you complimentary identity monitoring services for one year through Kroll.

Kroll is a global leader in risk mitigation and response and has extensive experience helping individuals who have had an unintentional exposure of personal information.

Visit [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) to activate and take advantage of your identity monitoring services.

You have until [Date] to activate your identity monitoring services.

Membership Number: <<Member ID>>

The services include: Web Watcher, Fraud Consultation, and Identity Theft Restoration services. Please see the additional information from Kroll included in this letter for further details about the identity monitoring services we are offering to you at no cost.

To activate your complimentary services, please go to [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) and using the Membership Number provided above. Please note that you must activate the services no later than [DATE].

**What You Can Do:** You can follow the recommendations on the following page to help protect your personal information.

**For More Information:** Further information about how to help protect your personal information appears on the following page. If you have questions concerning this incident, please contact our dedicated call center at 1-???-???-???? Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Sandi Jurek  
General Manager

## Steps You Can Take to Further Protect Your Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 (the "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 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 can also contact one of the following three national credit reporting agencies:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>	<b>Free Annual Report</b>
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>	<a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a>

**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 one (1) 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:** Under U.S. law, 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. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

<b>New York Attorney General</b>	<b>Maryland Attorney General</b>	<b>North Carolina Attorney General</b>	<b>Rhode Island Attorney General</b>
Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 <a href="mailto:ifraud@ag.ny.gov">ifraud@ag.ny.gov</a> 1-212-416-8433	200 St. Paul Place Baltimore, MD 21202 <a href="http://www.oag.state.md.us">www.oag.state.md.us</a> 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 <a href="http://www.ncdoj.gov">www.ncdoj.gov</a> 1-877-566-7226	150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">www.riag.ri.gov</a> 401-274-4400

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

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

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

### **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.

### **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.