

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
scottkev@gtlaw.com

September 1, 2022

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Formella:

We represent Legacy Supply Chain (“LSC”) located at 2001 Commerce Parkway, Franklin, IN 46131, and are writing to notify your office of an incident that may affect the security of some personal information relating to 19 New Hampshire residents.


On August 5, 2022, LSC discovered an unknown intruder had accessed its IT environment and, while the attack was quickly isolated and the intruder ejected from the environment, it was discovered on August 10, 2022, that the intruder may have accessed a server containing HR information including current and former employees' names, addresses, Social Security numbers, pay and direct deposit information. The investigation of the attack is ongoing.

LSC is taking steps to prevent a reoccurrence, to include measures to reduce the likelihood of a future cyberattack, including increased network security measures and employee training to recognize external attacks. LSC is also offering all potentially affected individuals 24 months of complimentary credit monitoring and identity theft restoration from Kroll.

On or about September 1, 2022, LSC began mailing notifications to all potentially affected individuals. An example of the notification is attached. Notification has also been made to the three major credit reporting agencies.

Should you have any questions regarding this notification or other aspects of the data security event, please contact me for any additional information.

Best Regards


Shareholder



<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you of a recent data security incident that may have impacted some of your personal information. We take the security of your information very seriously, and we sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to help protect your information.

What Happened?

As you may be aware, we were recently the target of a sophisticated cyberattack. The attacker gained access to our IT systems, with the intent to launch a much larger attack. We took immediate action to isolate the attack, secure our IT environment, and investigate the incident to withstand attempted future attacks. We also reported the attack to law enforcement. As a result of our investigation, we determined that the personal information of current and former employees may have been accessed by the attackers.

What information was involved?

As internal systems came back online, and our investigation led by a third-party cyber security vendor continued, we discovered that the attackers exfiltrated some data which included, among other things, personal information, including your name, address, Social Security number, pay and direct deposit information.

What We Are Doing

We take the security of your information seriously and are taking measures to reduce the likelihood of a future cyberattack, including increased network security measures and employee training to recognize external attacks. In addition, out of an abundance of caution, we are offering identity monitoring services through Kroll at no cost to you for two years. 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 confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$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(activation deadline)>> 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.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

What You Can Do

Please review the enclosed "Important Additional Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC), regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information

If you have questions, please call [1-800-800-8000](tel:1-800-800-8000), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting personal information is of the utmost importance to us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Mike Glodziak
President & CEO

(Enclosure)



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.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$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.

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**DC
Attorney General**
441 4th St NW
Washington, DC 20001
1-202-727-3400
www.oag.dc.gov

**Maryland Office of
Attorney General**
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**New York
Attorney General**
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

**North Carolina
Attorney General**
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

**Rhode Island Office
of Attorney General**
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf)), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.experian.com/freeze/center.html
1-800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com/credit-freeze
1-800-680-7289