January 23, 2025

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Anthony G. Brown,

We are writing to notify you of a cybersecurity incident that may have impacted certain individuals' personal information maintained by Logista Advisors, LLC ("Logista") as a result of unauthorized access by a third party to certain systems within Logista's information technology network. This incident may have involved personal information maintained by Logista related to three (3) Maryland residents. At this time, we have no indications that the personal information has been subject to fraudulent use as a result of this incident.

On or about August 7, 2024, Logista became aware that an unauthorized third party accessed its information technology network, encrypted certain systems, and exfiltrated certain data. Upon becoming aware of the incident, Logista retained leading experts, notified federal law enforcement, and implemented measures to assess and contain the incident. The incident has been contained.

The investigation has determined that an unauthorized third party exfiltrated certain data from certain Logista systems. We conducted a review of the potentially impacted data, which was completed as of December 30, 2024. Based on that review, we determined that the personal information of your state residents may have been impacted. The potentially impacted information includes driver's license number, passport number, and social security number. A sample individual notice is enclosed, which will be sent to each potentially impacted individual.

As an added precaution, Logista is offering the potentially impacted individuals complimentary access to twenty-four (24) months of credit monitoring, web monitoring, and identity theft restoration services.

If you have any questions, please do not hesitate to contact me at lvillarreal@logistacapital.com.

Sincerely

Lacie Villarreal

Lacie Villarreal
Chief of Staff
Logista Advisors, LLC

Logista

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

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

Notice of Data Breach

Dear <<first_name>> <<last_name>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident. At this time, we have no indication of fraudulent use of your personal information as a result of this incident.

What happened?

On or about August 7, 2024, Logista became aware that an unauthorized third party accessed its information technology network, encrypted certain systems, and exfiltrated certain data. Upon becoming aware of the incident, Logista retained leading experts, notified federal law enforcement, and implemented measures to assess and contain the incident. The incident has been contained.

The investigation has determined that an unauthorized third party exfiltrated certain data from certain Logista systems. As part of the review of the potentially impacted data, Logista identified that some of your personal information may have been among that data.

The Company has taken steps to further secure its systems, including, among other things, deploying additional security enhancements. The Company has also arranged to offer affected individuals access to credit monitoring, web monitoring, and identity theft restoration services.

What information was involved?

Based on our investigation, we understand that your <<b2b_text_1 (Data Elements)>> may have been obtained by the unauthorized third party**.**

What we are doing.

Upon becoming aware of the incident, we promptly launched an investigation, retained leading experts, and notified federal law enforcement. We also took measures to further secure our systems. The incident has been contained.

We have also secured the services of Kroll to provide identity monitoring at no cost to you for twenty-four (24) 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 confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. To activate these services, please take the following steps:

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.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call <<1-???-???-????>>, 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 your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Andrew Serotta
CEO

ADDITIONAL RESOURCES

Reviewing Your Accounts and Credit Reports. Regulators recommend that you be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution. As part of staying vigilant, you should regularly review your account statements for unauthorized activity, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	**Experian**	**TransUnion**
Credit Report: 1-800-685-1111 Fraud Alert: 1-800-525-6285 Equifax.com Equifax Credit Report, P.O. Box 740241, Atlanta, GA 30374 Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	1-888-397-3742 Experian.com Experian Credit Report, P.O. Box 2104, Allen, TX 75013 Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	Credit Report: 1-800-888-4213 Fraud Alert: 1-800-680-7289 Transunion.com Trans Union Credit Report, P.O. Box 2000, Chester, PA 19016 TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. A fraud alert tells lenders that they should verify your identification before they extend credit in your name. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Security Freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft. If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps.

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338). You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-919-716-6000.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

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

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

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

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also 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.

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.