PIERSON FERDINAND

TONY ONORATO
PARTNER

Mail
41 Front Street, 2nd Floor
Rockville Centre, NY 11570

Office
1270 Avenue of the Americas
7th Floor – 1050
New York, NY 10020

Direct: 202.459.3599
Facsimile: 516.706.9809
Email: tony.onorato@pierferd.com

March 12, 2024

VIA EMAIL (consumer@ag.iowa.gov)
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319

Re: Data Security Incident

Dear Attorney General Bird:

Pierson Ferdinand LLP represents Gerson Lehrman Group, Inc. ("GLG") located at 60 East 42nd Street, 3rd Floor, New York, NY 10165, in connection with a data security incident described in more detail below. The protection and proper use of information in its possession is a top priority for GLG and GLG has taken steps to prevent a similar incident from occurring again in the future.

1. Description of the incident

GLG experienced a ransomware incident in which an unauthorized third party accessed data from GLG's computer system. GLG immediately activated its incident response plan, engaged a national cybersecurity firm to assist in assessing the scope of the incident, retained additional cybersecurity experts to aid in reviewing and revising its security protocols and to harden its systems, and took steps to mitigate the potential impact of the incident. GLG has worked diligently to determine what happened and what information was involved as a result of this incident.

Following an investigation by third-party forensic specialists, data mining was conducted to identify the potentially impacted individuals and what elements of personally identifiable information may have been affected, and further efforts were made to locate address information for potentially impacted individuals. The investigation and data mining determined that the following elements of personal information of Iowa residents were potentially impacted as a result of this incident: name and Social Security number.

GLG has no indication that any personal information has been or will be used inappropriately.

2. Steps taken

Upon discovery, GLG reported the incident to federal law enforcement, and worked with cybersecurity counsel and forensic experts to investigate how the incident occurred and what information may have been impacted. GLG took appropriate remedial and hardening steps, including without limitation: updating and enhancing user access credentials and controls; implementing new technical safeguards; reviewing policies and procedures; and retraining workforce members.

Potentially impacted Iowa residents are being mailed notification letters on March 12, 2024. These letters include complimentary identity theft and credit monitoring services for twelve (12) months through CyEx Identity Defense Total.

3. Contact information

GLG remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at tony.onorato@pierferd.com or (202) 459-3599.

Sincerely,

Tony Onorato
Partner, Pierson Ferdinand LLP

EXHIBIT A

GLG

Return mail processing
P.O. Box 3826
Suwanee, GA 30024

Via First-Class Mail

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

<<Variable Header/Variable Data 2>>

Dear <<Full Name>>:

Gerson Lehrman Group ("GLG") recently experienced a data security incident that may have affected your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately. We nevertheless wanted to make you aware of the incident and the measures we have taken in response, as well as provide details on the steps you can take – should you deem it appropriate – to help protect your information. The protection and proper use of your information is a top priority for GLG, and we are working to prevent a similar incident from occurring again in the future.

What Happened

On November 12, 2023, GLG experienced a ransomware incident in which an unauthorized third party accessed data from GLG's computer system. We immediately activated our incident response plan, engaged a national cybersecurity firm to assist in assessing the scope of the incident, retained additional cybersecurity experts to aid us in reviewing and revising our security protocols and to harden our systems, and took steps to mitigate the potential impact of the incident. Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident. <<Variable Data 3 (The forensic investigation further determined that the incident potentially impacted approximately <<RI Count>> (<<R1 Count>>) Rhode Island residents.>>

What Information Was Involved

The elements of your personal information that might have been impacted include: name, <<Breached Elements>>. Please note that we have no evidence at this time that any of your personal information has been or will be misused as a result of the incident.

What We Are Doing

We are taking this incident very seriously and are committed to strengthening our systems' security to prevent a similar event from occurring in the future. Additionally, out of an abundance of caution, we have arranged for you to activate, at no cost to you, CyEx's Identity Defense Total credit monitoring services. These services provide you with alerts when changes occur to your credit file for <<CM Duration>> months from the date of enrollment. Additional information regarding CyEx Identity Defense Total credit monitoring services is found in the attachment to this letter.

What You Can Do

To enroll in the complimentary services we are offering you, please follow the instructions provided below. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter.

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Please note that certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at 888-318-4754 between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays, and are available for ninety (90) days from the date of this letter to assist you with questions regarding this incident.

Sincerely,

Gemma Postlethwaite

Gemma Postlethwaite, Chief Executive Officer
Gerson Lehrman Group

Identity Defense Total

Key Features

- 3-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/gers

1. Enter your unique Activation Code: **<<Activation Code>>**

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After **<<Enrollment Deadline>>**, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

Additional Important Information

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); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, 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 located below.

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

Security Freeze: You 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. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

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

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed below.

Implementing an Identity Protection PIN (IP PIN) with the IRS:
To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.
If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.
Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Iowa*, *Oregon*, and *West Virginia*: 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 https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

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

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

For residents of *Rhode Island*: You can obtain a police report if you are a victim of identity theft as well as obtain additional information from the Federal Trade Commission and the Rhode Island Office of the Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft at: Rhode Island Office of the Attorney General, Consumer Protection, 150 South Main Street, 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.ftc.gov/idtheft