



PIERSON FERDINAND

MICHAEL E. KAR
PARTNER

Rockefeller Center
1270 Avenue of the Americas
7th Floor
New York, NY 10020

July 22, 2024

Direct: 1.631.215.3415
Email: michael.kar@pierferd.com

Via Email (idtheft@oag.state.md.us)

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

Re: Data Security Incident

Dear Attorney General Brown:

Pierson Ferdinand LLP represents Green Investment Management, Inc. (“GIM”) located at 500 W 7th Street, Suite 827, Fort Worth, TX 76102, 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 GIM, and GIM has taken steps to prevent a similar incident from occurring again in the future.

1. Incident Description

GIM experienced a data security incident in which an unauthorized third party compromised GIM’s email and network environment. GIM secured and remediated the compromise, engaged additional third-party experts, enhanced our data security, and commenced an investigation.

The investigation determined that certain client files containing personal or financial information could have been compromised. Impacted data elements vary for each individual – the following personal information for your state’s residents could have been impacted by this incident: full name, Social Security number, and date of birth.

2. Steps taken

GIM is committed to ensuring the security and proper use of all information in its control. GIM worked with experts to investigate how the incident occurred and take appropriate remedial and hardening steps to enhance network security and data privacy. GIM notified law enforcement regarding this incident.

Notification letters were mailed to residents of your state on July 16, 2024. A sample copy of the notification letters is attached as Exhibit A. This notification included complimentary credit monitoring and identity protection services for twelve (12) months through CyEx, a company specializing in fraud assistance and remediation services. At this time, GIM is not aware of anyone experiencing fraud as a result of this incident.



PIERSON FERDINAND

Page 2 of 3

3. Contact information

GIM 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 michael.kar@pierferd.com or +1(631) 215-3415.

Sincerely,

Michael E. Kar
Partner, Pierson Ferdinand LLP

Enclosure (1)



PIERSON FERDINAND

EXHIBIT A



GREEN INVESTMENT MANAGEMENT, INC.

Secure Processing Center
P.O. Box 2623
Duluth GA 30096-9998



July 16, 2024

Notice of Data Incident

Dear [REDACTED],

Green Investment Management, Inc. ("GIM") recently detected a compromise to its network environment that could have affected your personal or financial information. We have no indication that your information has been or will be misused. We want to make you aware of the incident and the measures we have taken in response, as well as provide details on steps you can take – should you deem it appropriate – to help protect your information. The protection, privacy, and proper use of your information is paramount, and we are working to prevent this type of incident from occurring again.

What Happened

GIM identified unauthorized activity in its email environment. We secured and remediated the compromise, engaged additional third-party experts, enhanced our data security, and commenced an investigation. We have worked diligently to determine what happened and what information could have been compromised. Unfortunately, these types of incidents have become increasingly common and even organizations with the most sophisticated IT infrastructure available are affected.

What Information Was Involved

The third-party digital forensic investigation determined that your personal or financial information was subject to unauthorized activity. While the impacted data elements vary, this could have included: full name, [REDACTED]. GIM is not aware of any fraud occurring as a result of this incident.

What We Are Doing

We take this incident seriously and are committed to continuing to strengthen our systems' security to prevent a similar event from occurring in the future. We are also focused on enhancing our cyber preparedness through additional awareness training and updating our procedures. GIM notified law enforcement regarding this incident.

Additionally, out of an abundance of caution, we have arranged for you to activate complimentary credit monitoring and identity restoration services for [REDACTED] months through CyEx. These services will be provided by CyEx, a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the complimentary services we are offering you, please follow the instructions provided. For you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. You can enroll by using enrollment code [REDACTED] and visiting app.identitydefense.com/enrollment/activate/gimi.

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. We encourage you to review the [Additional Important Information](#) located on the following pages, which includes further steps to safeguard your personal information, such as implementing a fraud alert or security freeze. We also recommend validating the sender of any emails and being wary of phishing attempts.

For More Information

Please know that Green Investment Management values the protection and privacy of your personal information, and we understand the concern and inconvenience this incident may cause. If you have any questions, call 888-596-6087 between 9:00 AM and 9:00 PM ET, Monday through Friday, excluding holidays.

Sincerely,

A handwritten signature in black ink, appearing to read 'Byron Green', with a stylized flourish at the end.

Byron Green
President
Green Investment Management, Inc.

Additional Important Information

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. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. 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 get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit www.annualcreditreport.com; call, toll-free, 1-877-322-8228; or mail 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.

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 may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. 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:

<u>Experian</u>	<u>Equifax</u>	<u>TransUnion</u>
1-888-397-3742	1-800-349-9960	1-888-909-8872
www.experian.com/help/	www.equifax.com/personal/credit-report-services/	www.transunion.com/credit-help
<u>Fraud Alert</u> P.O. Box 9554 Allen, TX 75013	<u>Fraud Alert</u> P.O. Box 105069 Atlanta, GA 30348-5069	<u>Fraud Alert</u> P.O. Box 2000 Chester, PA 19016
<u>Credit Freeze</u> P.O. Box 9554, Allen, TX 75013	<u>Credit Freeze</u> P.O. Box 105788 Atlanta, GA 30348-5788	<u>Credit Freeze</u> P.O. Box 160, Woodlyn, PA 19094

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. 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 and validate your identity. Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Fair Credit Reporting Act: 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/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

For Massachusetts residents: You can obtain a police report if you are a victim of identity theft.

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

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

For Vermont residents: 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).

Residents of the below states can obtain additional information regarding identify theft and more at:

- **District of Columbia Attorney General:** 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.
- **Maryland Office of the Attorney General:** Consumer Protection Division, 200 St. Paul Place, 16th Fl, Baltimore, MD 21202; 1-888-743-0023; <https://www.marylandattorneygeneral.gov/>.
- **New York Attorney General:** Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.
- **North Carolina Attorney General:** 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.