Stirlingshire BD LLC
15 W 38th St. #704
New York, New York 10018

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

November 15, 2024

RE: Notice of Data Breach
Please read this entire letter

Dear <<First Name>> <<Last Name>>:

As you may be aware, Stirlingshire BD LLC ("Stirlingshire") recently experienced a data security incident that may have impacted some of your personal information. We take the security of your personal information very seriously, and we sincerely regret having to share this news with you. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
Beginning on or about September 4, 2024, an unauthorized third party gained access to an employee's Stirlingshire account. The access enabled them to view certain emails in the employee's mailbox and, on October 4, 2024, gain access to our investment platform. While we cannot determine specifically if the unauthorized third party viewed accounts of all of our clients, because we cannot rule out the possibility, we are notifying you. We became aware of the incident on October 11, 2024, and launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. We completed our investigation on October 24, 2024.

What Information Was Involved?
Through our investigation, we learned that certain data may have been viewed without authorization. This data includes your name, your primary email, account number and type, your primary phone number, and the last four digits of your social security number.

What We Are Doing
Stirlingshire takes the security of all information in our systems very seriously, and we want to assure you that we've already taken decisive steps to prevent a reoccurrence. Upon discovery, we quickly contained the incident by decoupling the platform's direct access to the markets and eradicating the unauthorized third party from our systems, including the mailbox. Among other actions, we have increased monitoring, further improved security controls, and reinforced our systems.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do
We recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information.

We encourage you to contact IDX to enroll in free identity protection services by calling (833) 903-3648, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 15, 2025.

For More Information
If you would like to request any additional information about this incident, please contact us at info@stirlingshire.com, 1-877-600-7026, or mail at 15 W 38th St. #704 New York, NY 10018. Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Stirlingshire BD LLC

Additional Important Information

Monitoring: For at least the next twelve to twenty-four months, you should 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 and immediately report any suspicious activity or incidents of identity theft to the financial institution or company with which the account is maintained. You have the right to obtain or file a police report. You can contact the Federal Trade Commission for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the Federal Trade Commission.

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

Credit Reports: 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. We recommend that you request that any information relating to fraudulent transactions be deleted from your report. 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 have the right to place free fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.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. To protect against fraud, we recommend that you periodically obtain credit reports from each of the three nationwide credit bureaus, though they may not be free.

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. For that reason, placing a security freeze can protect you, but also may delay you when you seek to obtain credit. 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.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

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

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

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

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, for the next twelve to twenty-four months 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.

For residents of District of Columbia, Maryland, New York, and North Carolina:
You can obtain information from the District of Columbia, Maryland, North Carolina, and New York 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
400 6th Street NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

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
https://ncdoj.gov/