KESTRA
INVESTMENT SERVICES

5707 Southwest Parkway, Bldg. 2, Ste. 400, Austin, Texas 78735 844-5-KESTRA (844-553-7872)

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED
DEC 21 2018
CONSUMER PROTECTION

December 20, 2018

VIA OVERNIGHT (FEDEX 774030096618)

To Whom It May Concern:

I am writing on behalf of Kestra Investment Services, LLC ("Kestra") to notify you of a security incident involving New Hampshire residents.

Kestra utilizes the services of Capital Forensics, Inc. ("CFI"), for regulatory compliance support services. On or about November 1, 2018 CFI was the victim of a malicious cyberattack. This attack resulted in an unauthorized person gaining access to a single CFI user's account on a third party file-sharing system it uses to share data with customers, including Kestra. CFI cut off access to the account within four hours of the incident's occurrence, and the incident was fully mitigated within six hours. CFI reported that files containing Kestra client information were among the data potentially accessed. Kestra immediately undertook an internal investigation and on November 21, 2018 determined that personally identifiable information for Kestra clients and participants in retirement plans serviced by Kestra was compromised.

On December 20, 2018, Kestra began mailing written communications to impacted individuals, including 33 residents of New Hampshire, in substantially the same form as the enclosed letter.

CFI is offering the impacted individuals a complimentary two-year membership in credit monitoring and identity theft protection services through AllClear. In addition, AllClear is providing a toll-free number impacted individuals can call with any questions or concerns they may have.

Kestra continues to investigate the incident in order to determine what, if any, additional safeguards could be employed to reduce the likelihood of similar occurrences with its vendors in the future.

Please do not hesitate to contact me with any questions you may have,

Sincerely,

Michael Pedlow, Chief Compliance Officer
Kestra Investment Services

Kestra Financial, Inc is the parent company of Kestra Investment Services, LLC member FINRA/SIPC.

KESTRA
INVESTMENT SERVICES
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
R83480A

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 20, 2018

NOTICE OF DATA BREACH

Dear John Sample,

We are writing on behalf of Kestra Investment Services, LLC (Kestra IS) to inform you of an incident that may have involved some of your personal information. You're receiving this notice because our records show you are or were a client of Kestra IS or a participant in a retirement plan serviced by Kestra IS. We take the protection of your personal information seriously, and want to inform you about what we have done to address this data breach and what steps you can take to protect yourself at no cost to you.

What Happened?
Kestra IS utilizes the services of a well-respected third party service provider, Capital Forensics, Inc. (CFI) for regulatory compliance support, including the review of accounts for such purpose. CFI discovered that an unauthorized third party accessed data files through a file sharing system CFI used with their clients. The unauthorized third party appears to have gained access to data files through a CFI employee account, and the files contained personally identifiable information.

Once notified, Kestra IS conducted a forensic analysis to determine who was impacted. On November 21, 2018 we determined that your information may have been compromised.

What Information Was Involved?
The personal information we currently believe to have been compromised includes some or all of the following: first and last names, Social Security number, and account number.

What We Are Doing.
CFI promptly acted to secure the compromised account and notified law enforcement. CFI also engaged an independent forensic investigation firm to conduct an analysis of the data breach. Kestra IS and CFI continue to investigate the incident to ensure the appropriate steps have been taken.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months. There are two types of protection available:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-263-9943 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service requires enrollment and offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-263-9943 and using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

What You Can Do.
We want to make you aware of steps you may take to guard against identity theft or fraud. In addition to enrolling in the AllClear ID services above, please review the enclosed "**Additional Actions to Help Reduce Your Chances of Identity Theft**" for simple, no-cost steps you can take to help protect against the possibility of identity theft.

For More Information.
We sincerely apologize for any inconvenience or concern caused by this incident. If you have questions or concerns about this incident, please contact our dedicated call center at 1-855-263-9943 Monday – Saturday 8am – 8pm Central Time (excluding national holidays).

Sincerely,

Mike Pedlow, Chief Compliance Officer
Kestra Investment Services, LLC
5707 Southwest Parkway
Bldg 2 Suite 400
Austin, TX 78735

Additional Actions to Help Reduce Your Chances of Identity Theft

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call (877) 322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ USE TOOLS FROM CREDIT PROVIDERS

We recommend you remain vigilant for instances of fraud and identity theft. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Security freezes must be placed separately for each of the credit reporting companies. To place a security freeze on your credit report, you must send a separate request to **each** of the three major consumer credit reporting agencies (Equifax, Experian, and TransUnion) online, by telephone, or by regular, certified, or overnight mail as provided below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 685-1111
For NY Residents: (800) 349-9960
https://www.equifax.com/personal/credit-report-services/

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

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8800
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)

The credit reporting agencies have three (3) business days after receiving your request by mail, or one (1) business day if requested by toll-free telephone or secure electronic means, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To temporarily lift the security freeze in order to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies through their websites, via telephone, or by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request by mail, or one (1) hour if requested by toll-free telephone or secure electronic means, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must contact each of the three credit bureaus through their websites, by telephone (where permitted), or by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request by mail, or one (1) hour if requested by toll-free telephone or secure electronic means, to remove the security freeze.

➢ PLACE A FRAUD ALERT ON YOUR CREDIT FILE

There are two types of fraud alerts that 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. An **initial fraud alert** stays on your credit report for at least 90 days, while an **extended fraud alert** stays on your credit report for seven years and may be placed on your credit report if you have already been a victim of identity theft and have the appropriate documentary proof. A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud or identity theft. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of with whom you are sharing your personal information and shredding receipts, statements, and other sensitive information.

➢ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You may obtain more information from the Federal Trade Commission (FTC) about steps you can take to avoid identity theft, including how to place a fraud alert or security freeze on your credit file. The FTC may be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580.
ID Theft hotline: (877) IDTHEFT (438-4338)
www.ftc.gov
www.identitytheft.gov

➢ REDUCE THE RISK OF TAX-RELATED FRAUD

To reduce the risk of tax-related fraud, you may contact the IRS Identity Protection Specialized Unit at (800) 908-4490 (Monday through Friday, 7:00 am – 7:00 pm local time). The IRS also provides identity theft-related resources at https://www.irs.gov/identity-theft-fraud-scams/identity-protection. You may also want to contact your state tax authority and tax advisors to notify them of the potential for identity theft and to protect against the possibility of a fraudulent tax return.

➢ RESIDENTS OF IOWA

Iowa residents are advised to report any suspected incidents of identity theft to the Attorney General or to local law enforcement. The Attorney General may be contacted at:

Iowa Office of the Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319

(888) 777-4590 (toll-free in Iowa)
(515)-281-5926
consumer@iowa.gov
www.iowaattorneygeneral.gov

➢ RESIDENTS OF MARYLAND

Maryland residents can obtain information from the Maryland Attorney General about steps they can take to avoid identity theft at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
Consumer@oag.state.md.us
www.oag.state.md.us

➢ RESIDENTS OF MASSACHUSETTS

Under Massachusetts law, you have a right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. See above for details on security freezes, including how to place, temporarily lift, or permanently remove a security freeze on a credit report. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, that credit reporting agency cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

➢ RESIDENTS OF NEW MEXICO

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your files at consumer reporting agencies; to dispute incomplete or inaccurate information in your files at consumer reporting agencies; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information in your credit file. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or the FTC website at www.ftc.gov.

In addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. the unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. proper identification to verify your identity;
3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

➢ RESIDENTS OF NORTH CAROLINA

North Carolina residents can obtain information from the North Carolina Attorney General about steps they can take to avoid identity theft at:

North Carolina Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov/Consumer.aspx

➢ RESIDENTS OF OREGON

Oregon residents are advised to report any suspected incidents of identity theft to law enforcement, including the Oregon Attorney General and the Federal Trade Commission. The Oregon Attorney General may be contacted at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
www.doj.state.or.us

Oregon Consumer Protection Hotlines
Salem: (503) 378-4320
Portland: (503) 229-5576
Toll-Free: (877) 877-9392
help@oregonconsumer.gov

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077