BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Gerald J. Ferguson
direct dial: 212.589.4238
gferguson@bakerlaw.com

September 3, 2020

VIA OVERNIGHT MAIL

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, the Integrity Wealth Management, ("IWM"), to notify you of a security incident. IWM is a financial services organization that specializes in employer sponsored investment products. Securities are offered through Kestra Investment Services, LLC, a registered broker/dealer, and advisory services are offered through Kestra Advisory Services, LLC, a registered investment adviser (collectively "Kestra"). Kestra has been made aware of this matter and are participating in the response plan with a goal toward the protection of relevant client data.

Some of the data that was the subject of this investigation was data owned by IWM's corporate clients. Those corporate clients were notified of this incident beginning in August 2020. This notice is on behalf of IWM, Kestra and one of IWM's corporate client: Med Speed LLC.

On April 16, 2020, IWM received reports from clients and other contacts that a suspicious email was received from one of IWM's employees. Upon learning this, IWM notified its broker-dealer and retained Baker & Hostetler, LLP ("BakerHostetler") to provide legal advice and assistance investigating and responding to the incident. BakerHostetler, on behalf of IWM, engaged cybersecurity professionals to conduct a forensic investigation to allow BakerHostetler to provide legal advice to IWM.

On May 7, 2020, the forensic investigation confirmed unauthorized access to a single IWM employee's email account. The investigation was unable to determine which emails or

attachments may have been accessed or viewed by the unauthorized party. Out of an abundance of caution, IWM reviewed the emails and attachments in the employee's email account to identify any personal information. On June 27, 2020, the review was completed and IWM determined that there were documents containing personal information of employees of its corporate clients as well as information related to direct clients of IWM. The information included individual names, financial account numbers, Social Security numbers, driver's license numbers or state identification numbers, and username and password information for online accounts. IWM notified one New Hampshire resident of this incident.

On August 28, 2020, IWM mailed notification letters via United States Postal Service First Class Mail to the one New Hampshire resident in accordance with N.H. Rev. Stat. § 359-C:20.[1] A sample copy of the notification letter is enclosed. IWM has established a dedicated call center where all individuals may obtain more information regarding the incident. Notification of this incident is being provided as quickly as possible, following the completion of the investigation, which was performed without unreasonable delay, despite significant challenges due to the COVID-19 pandemic.

To help prevent a similar incident from occurring in the future, IWM implemented additional security measures. In addition, IWM continues to cooperate with law enforcement to investigate this incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Gerald J. Ferguson
Partner

Enclosure

[1] This report is not and does not constitute a waiver of Integrity Wealth Management's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

KESTRA
INVESTMENT SERVICES

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

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

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

Integrity Wealth Management values the relationship we have with our clients and we understand the importance of safeguarding personal information. <<b2b_text_1(NameofEmployer)>><<b2b_text_2(NameofEmployer)>>. We are writing to inform you of a security incident that we have identified and addressed that may have involved your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently concluded an investigation into an email phishing incident and determined that an unauthorized party accessed one of our employee email accounts. Upon learning of the phishing incident, we immediately took steps to secure the email account and began an investigation with the assistance of cybersecurity professionals. The investigation determined that an unauthorized party accessed the employee's email account on April 16, 2020.

The investigation was not able to determine which emails or attachments, if any, were viewed by the unauthorized party. Out of an abundance of caution, we conducted a review of emails and attachments in the employee's email account and determined on June 27, 2020, that an email or attachment contained your name and one or more of the following data elements: financial account number(s), Social Security number, driver's license or state identification number, and/or a username and password to an online account.

Although, to date, we have no evidence that your information has been misused, we assure you that we take this incident very seriously. As a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

While we have no evidence at this time that your information was actually viewed by the unauthorized person, or that it has been misused, we encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. For some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We regret this incident occurred and apologize for any inconvenience. We have implemented additional security measures to help prevent a similar incident in the future. If you have any questions, please call 1-???-???-????, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time.

Sincerely,

William J. Cronin
Managing Partner
Integrity Wealth Management
20975 Swenson Drive, Suite 225
Waukesha, WI 53186

Todd R. Kreitzman
Managing Partner
Integrity Wealth Management
20975 Swenson Drive, Suite 225
Waukesha, WI 53186

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission,* Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will 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.

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.