Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 11, 2020

**VIA E-MAIL**

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent CorePower Yoga, LLC ("CorePower") located at 3001 Brighton Boulevard, Suite 269, Denver, CO 80216 and are writing to notify your office of an incident that may affect the security of some personal information relating to five hundred fifty-nine (559) Washington residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CorePower Yoga does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

## Nature of the Data Event

CorePower previously became aware of suspicious activity occurring within an employee's email account, CorePower changed the employee's email account password and commenced an investigation to identify the source of the activity. As part of the investigation into the incident, which was conducted with the assistance of a third-party forensic specialist, it was determined that multiple employee email accounts were subject to unauthorized access between November 7, 2019 and February 3, 2020. The investigation was unable to determine which, if any, emails and attachments within the email accounts were accessed or viewed.

The forensic specialist completed its analysis of the email accounts on August 13, 2020 and prepared a list of individuals whose information was determined to be present in the emails or attachments located in the email accounts and possibly viewed by the unauthorized party. The data elements potentially affected include, Social Security number, driver's license and/or state identification number, credit and/or debit card number, passport number, medical information, health insurance information, and date of birth.

## Notice to Washington Residents

On September 11, 2020, CorePower Yoga provided written notice of this incident to affected individuals, which includes approximately five hundred fifty-nine (559) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A*.** CorePower Yoga may supplement this notification if it is determined that a significant amount of additional Washington residents will require notice.

## Other Steps Taken and To Be Taken

Upon discovering the event, CorePower Yoga moved quickly to investigate and respond to the incident, assess the security its systems and notify potentially affected individuals. CorePower also changed employee account passwords at issue, reviewed existing security measures, and is working diligently to implement additional security measures to ensure the security of their network.

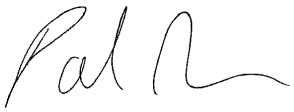
CorePower Yoga is not aware of any attempted or actual misuse of personal information. Additionally, CorePower Yoga provided impacted individuals with twelve (12) months of free credit monitoring, guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

CorePower Yoga takes this matter and the confidentiality, integrity, and security of the personal information in its care, seriously and has taken measures to minimize the risk of a similar future data incident. CorePower Yoga is committed to ongoing employee training designed to help them identify and properly report potential email phishing scams. These measures also include a review of CorePower Yoga's policies and procedures relating to the security and confidentiality of CorePower Yoga's records containing personal information. CorePower Yoga will also provide notice of this incident to the impacted individuals, other state Attorneys General, and consumer reporting agencies, where required.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,



Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/mef

# EXHIBIT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

CorePower Yoga, LLC ("CorePower") is writing to make you aware of a recent data privacy event that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

***What Happened?*** CorePower previously became aware of suspicious activity occurring within an employee's email account, changed the employee's email account password. and commenced an investigation to identify the source of the activity. As part of the investigation into the incident, which was conducted with the assistance of a third-party forensic specialist, it was determined that multiple employee email accounts were subject to unauthorized access between November 7, 2019, and February 3, 2020. The investigation was unable to determine which, if any, emails and attachments within the email accounts were accessed or viewed. Therefore, the forensic specialist then undertook a time-consuming review of all the emails and attachments in the email accounts to determine whether they contained any sensitive information.

The forensic specialist completed its analysis of the email accounts on August 13, 2020, and prepared a list of individuals whose information was determined to be present in the emails or attachments located in the email accounts and possibly viewed by the unauthorized person(s).

***What Information is Involved?*** The information related to you found within the email account includes your name and <<Breached Elements>>. We were unable to determine which emails, if any, in the accounts were subject to unauthorized access but are providing notice out of an abundance of caution as your information was contained within the email accounts subject to unauthorized access.

***What Are We Doing?*** We take the security of information entrusted to us very seriously and we apologize for the inconvenience this incident has caused you. We changed the CorePower employee account passwords at issue, reviewed existing security measures, and are working diligently to implement additional security measures to ensure the security of our network. We are also providing you with information about this event and about the steps you can take to protect your personal information, should you feel it appropriate to do so.

We are offering you access to twelve (12) months of free credit and identity monitoring through TransUnion.

***What You Can Do.*** We encourage you to monitor your credit card statements and other financial accounts closely and report any suspected fraud to your issuing bank. You can also review the enclosed "Steps You Can Take to Protect Your Information" for additional information about how you can protect your identity and on how to enroll in the free credit and identity monitoring services.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, we have set up a call center that you can reach at 888-490-0587, Monday through Friday, from 6:00 a.m. to 6:00 p.m. Pacific Time.

We apologize for any inconvenience this incident may have caused.

Sincerely,

CorePower Yoga, LLC

## *Steps You Can Take to Protect Your Information*

### Enroll in Credit Monitoring

See last page for instructions.

### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

You have the 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 control 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 may make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 9554 | P.O. Box 2000 | P.O. Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-800-680-7289 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

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 during the past five (5) years, the addresses where you have lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-800-525-6285 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For Maryland Residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

**For North Carolina Residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6000, www.ncdoj.gov.

**For New Mexico Residents**, The New Mexico Attorney General can be reached at 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, 1-844-255-9210, www.nmag.gov.

TransUnion

**Activation Code: <<Activation Code>>**

# Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

**How to Enroll: You can sign up online or via U.S. Mail delivery**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)