



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

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

November 10, 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 Woodruff Sawyer & Co. (“Woodruff Sawyer”) located at 50 California Street, Floor 12, San Francisco, CA 94111 and are writing on behalf of the below entities to notify your Office of an incident that may affect the security of some personal information relating to two thousand, three hundred and ninety-three (2,393) Washington residents. Woodruff Sawyer is an insurance consulting brokerage firm which includes services related to Workers’ Compensation claim consultation services for the following entity (“Client”) and includes the total number of impacted individuals in parenthesis below:

- United States Bakery, 315 NE 10th Ave, Portland, OR 97232 (2,393)

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, Woodruff Sawyer 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 Data Event

Woodruff Sawyer recently discovered suspicious activity related to certain employee email accounts. Upon learning of this activity, Woodruff Sawyer immediately took steps to secure the email accounts by changing the account credentials and launched an investigation, which included working with a third-party forensic investigator to determine the nature and scope of the activity.

This investigation determined that email account credentials were used by an unknown actor(s) to gain unauthorized access to certain employee email accounts. While the investigation confirmed the unauthorized actor(s) gained access to the email account on separate occasions between March 2, 2020 and March 3, 2020, the investigation was unable to identify all emails or attachments in the accounts that the unauthorized actor(s) may have had access to. As a result, Woodruff Sawyer, with the assistance of third-party forensics, quickly began a programmatic and manual review of the contents of the email accounts to determine the types of protected information present at the time of this activity and to which individuals the information relates. On or about September 1, 2020, this extensive review was completed, and Woodruff Sawyer immediately began a supplemental review its internal files in order to determine to which Woodruff Sawyer clients the information belonged. While this review is ongoing, Woodruff Sawyer notified Client of this incident because certain current and/or former employees related to them were identified during the review. The information that may have been subject to unauthorized access includes name, date of birth, diagnosis or symptom information, medical history/treatment information, and/or billing/claims information. Woodruff Sawyer is providing notice to impacted individuals and regulators, as required, on Client's behalf.

Notice to Washington Residents

On or about November 9, 2020, Woodruff Sawyer provided written notice of this incident which includes approximately two thousand, three hundred and ninety-three (2,393) Washington residents, is being provided in substantially the same form as the letter attached here as *Exhibit A*. Notification to impacted clients and individuals is ongoing, and Woodruff Sawyer may supplement this notification if it is determined that a significant amount of additional Washington residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Woodruff Sawyer moved quickly to investigate and respond to the incident, assess the security of Woodruff Sawyer's systems, and notify potentially affected individuals and Woodruff Sawyer clients. Woodruff Sawyer immediately reset the email account passwords, confirmed the security of relevant systems, reviewed policies and procedures, and has implemented additional safeguards and training to its employees including multi-factor authentication across the organization.

While Woodruff Sawyer is not aware of any attempted or actual misuse of personal information, it is providing the impacted individuals with access to twelve months (12) of credit and identity monitoring services, through Kroll, at no cost to these individuals.

Additionally, Woodruff Sawyer is and will be providing impacted individuals with 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

Office of the Attorney General

November 10, 2020

Page 3

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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,



Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/ara

EXHIBIT A



[Name]

[Address]

[Date]

Dear [NAME]:

Woodruff Sawyer & Co. (“Woodruff Sawyer”) is writing to inform you of a recent event that may impact the security of some of your personal information. Woodruff Sawyer received your information in connection with insurance consulting and brokerage services on behalf of your current or former employer, [Company Name]. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? Woodruff Sawyer recently discovered suspicious activity related to certain Woodruff Sawyer employee email accounts. We immediately took steps to secure the email accounts and launched an investigation which included working with a third-party forensic investigator to determine the nature and scope of the activity. The investigation determined that an email account belonging to a Woodruff Sawyer employee was subject to unauthorized access on separate occasions between March 2, 2020 and March 3, 2020. As a result, the unauthorized actor may have had access to certain emails and attachments within the account.

What Information Was Involved? The investigation was unable to identify all emails or attachments in the account that the unauthorized individual may have accessed or acquired. Therefore, in an abundance of caution, Woodruff Sawyer notified [Company Name] of this incident and conducted a review of the entire contents of the email account for emails or attachments that contain personal information. This review was completed on September 1, 2020 and we are notifying you of this incident because the investigation confirmed that the account may have contained your [VARIABLE TEXT FIELD]. To date, Woodruff Sawyer has not received any reports of actual or attempted misuse of your information.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we discovered this incident, we immediately reset the email account password and took steps to determine what personal information was in the account and to which Woodruff Sawyer clients the information belonged. We also confirmed the security of our employee email accounts and related systems. As part of our ongoing commitment to the security of personal information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We will also be notifying state and federal regulators, as required.

As an added precaution, we are offering you complimentary access to one year of credit and identity monitoring, fraud consultation and identity theft restoration services through Kroll. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. You may review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains general information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also enroll to receive the free credit and identity monitoring services we are offering.

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, please call Woodruff Sawyer at our dedicated assistance line at [phone number] between the hours of [XXX and XXX]. You may also write to Woodruff Sawyer at [INSERT MAILING ADDRESS].

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

[NAME]

[TITLE]

Woodruff Sawyer & Co.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

[VENDOR ENROLLMENT INFORMATION]

Monitor 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 free credit report annually from each of the three 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 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 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. 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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

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 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;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include 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 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 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional 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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are **XX** Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.