MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Sian M. Schafle
Office: 267-930-4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 22, 2018

VIA U.S. 1st CLASS MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

Our office represents Employee Benefits Corporation, headquartered at 1350 Deming Way, Suite 300, Middleton, Wisconsin 53562. We write to notify you, per the request of InterVarsity Christian Fellowship/USA, of an event reported to Employee Benefits Corporation. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Employee Benefits Corporation does not waive any rights or defenses it may have regarding the applicability of New Hampshire law or personal jurisdiction.

Background

Employee Benefits Corporation provides benefit administration services on behalf of employers. In the course of providing benefit administration services to its clients, Employee Benefits Corporation receives certain information on employees of its clients, who are participants of plans administered or serviced by Employee Benefits Corporation.

On March 7, 2018, Employee Benefits Corporation became aware of unusual FedEx tracking emails, which took the form of a typical phishing email, received by certain participants of benefit plans administered by Employee Benefits Corporation. While these emails did not originate from Employee Benefits Corporation, the emails did contain name, email address, and in some instances, a Social Security number, for participants present in a database on Employee Benefit Corporation's internal

systems. Employee Benefits Corporation immediately commenced an investigation, with the assistance of a third-party forensic investigation firm, to determine what happened and to confirm the security of Employee Benefit Corporation's internal systems.

In addition to name, the database may contain the following information about participants: email address, Social Security number, phone number, mailing address, date of birth, and in limited circumstances, financial account information and healthcare related information.

While the investigation confirmed that the information reported to be in the unusual emails exists together within a database on Employee Benefit Corporation's internal systems, the investigation did not identify a compromise in the security of this database. Due to the sensitive nature of the information in the unusual emails, out of an abundance of caution, on April 27, 2018, Employee Benefits Corporation provided notice to all clients with participant information contained within the database and offered to notify participants on behalf of its clients upon authorization to do so.

Notice to New Hampshire Residents

Employee Benefits Corporation received authorization from InterVarsity Christian Fellowship/USA to mail written notice of this event to their benefit plan participants whose information was contained in the database, including nine (9) New Hampshire residents.[1] On May 22, 2018, Employee Benefits Corporation, on behalf of this client, began mailing written notice of this event to these individuals in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon authorization to do so, Employee Benefits Corporation is notifying participants with information contained within the database. While no compromise of the security of the database was identified, out of an abundance of caution, Employee Benefits Corporation is offering those individuals one (1) year of complimentary credit monitoring and identity restoration services with TransUnion, in addition to helpful information on how to protect against identity theft and fraud. Employee Benefits Corporation is also cooperating with the Federal Bureau of Investigation's and state law enforcement's investigation into the unusual emails. In addition to providing notice of this event to your office, Employee Benefits Corporation will provide, on behalf of its clients, notice of this event to certain other state regulators, the U.S. Department of Health and Human Services, and the consumer reporting agencies upon authorization to do so.

[1] Because other entities have not yet responded to Employee Benefits Corporation's offer to notify participants whose data was contained within the database, additional residents may receive notice of this potential event. If so, Employee Benefits Corporation will supplement this notice.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS:ncl
Enclosure

EXHIBIT A

Employee Benefits Corporation
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>>:

Employee Benefits Corporation provides or previously provided <<Client>> with benefit administration services. In the course of providing these services, Employee Benefits Corporation received some of your personal information. We are writing to inform you, on behalf of <<Client>>, of a recent event reported to our organization.

What Happened? On March 7, 2018, Employee Benefits Corporation became aware of unusual FedEx tracking emails, which took the form of a typical phishing email, received by certain participants of a small number of benefit plans administered by Employee Benefits Corporation. While these emails did not originate from Employee Benefits Corporation, the emails did contain name, Social Security number (in some cases), and email addresses for individuals, which are present in a database on Employee Benefits Corporation's internal systems. Employee Benefits Corporation immediately launched an investigation with the assistance of a third-party forensic investigation firm to determine what may have happened and to confirm the security of our internal systems.

This extensive investigation did not indicate a compromise in the security of benefit plan participant data stored on our systems. However, we are notifying you, per <<Client>>'s request, because certain information relating to you is contained in the database storing participant data contained in the unusual emails.

What Information Was Involved? In addition to your name, the database may contain the following information about you: email address, Social Security number, phone number, mailing address, date of birth, and in limited circumstances, financial account information and healthcare related information.

What We Are Doing. Upon learning of the unusual emails, we moved quickly to investigate the event and confirm the security of our systems. In addition to providing notice of this event to <<Client>> and providing this notice to you, we are cooperating with the Federal Bureau of Investigation's and state law enforcement's investigations into the emails. While we've received no reports of identity fraud or identity theft, we are offering you access to 12 months of credit monitoring and identity restoration services with TransUnion. This offer is out of an abundance of caution and at no cost to you.

What You Can Do. You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*, which includes instructions on how to enroll in complimentary credit monitoring and identity restoration services, as well as information on what you can do to better protect against the possibility of identity theft and fraud.

For More Information. We understand you may have questions that are not answered in this letter. For more information please contact our call center staffed with individuals familiar with this event at 855-648-7638, Monday through Friday, 8:00 AM CT through 8:00 PM CT.

Sincerely,

Erin Freiberg, JD
Privacy Officer

Steps You Can Take to Protect Against Identity Theft and Fraud

Enroll in Credit Monitoring.

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.

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 following 12-letter Activation Code **<<Insert Unique 12- letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and **<<Insert Date >>.** 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.

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, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Insert static 6-digit Telephone Pass Code>>** to speak to a TransUnion representative about your identity theft issue.

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports and explanation of benefits forms 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.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation. **For Maryland residents,** the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Employee Benefits is located at 1350 Deming Way, Suite 300, Middleton, Wisconsin 53562. **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 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 by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents,** the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of <<Count>> Rhode Island resident[s] may be impacted by this incident.