MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 19, 2019

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Wescom Central Credit Union ("Wescom") located at 123 S. Marengo Avenue, Pasadena, California 91101, and write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Wescom does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

As a matter of background, Wescom contracts with a third-party vendor, Geezeo, to provide personal financial management tools to its customers. On or about September 24, 2019, Wescom was notified by Geezeo, regarding an incident that resulted in unauthorized acquisition of Wescom customer information. Geezeo reports that on May 14, 2019, an unauthorized party downloaded three legacy database backup files belonging to Geezeo and hosted through Amazon Web Services.

The impacted backup files contained historical Wescom member information dating from 2012. The information that could have been subject to unauthorized access includes name and financial account information including account number, account type, account balance (as of 2012), and user and account information. The files may have also contained member's financial information from non-Wescom accounts (which varied by impacted member). The exposed data did not contain any Social Security numbers, passwords, security codes, access codes, or other similar information that would allow access to Wescom members' accounts.

Notice to New Hampshire Resident

On or about November 19, 2019 Wescom provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Wescom began an investigation to determine the nature and scope of the incident, including identifying the individuals who may be affected, putting in place resources to assist them, and providing them with notice of this incident. Wescom was also informed that Geezeo implemented additional security measures to prevent this from happening in the future. Wescom and Geezeo have also notified appropriate authorities and regulators to ensure the incident is properly addressed.

Wescom is providing access to twelve (12) months of credit monitoring and identity restoration services through Equifax to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Wescom is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Wescom is providing individuals with 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

Enclosures
ATW/jsj

EXHIBIT A

WESCOM
Credit Union

November 19, 2019

P2 T33 Pk01 3340 ****AUTO**ALL FOR AADC 917
[FName LName]
[Street Address]
[Street Address 2]
[City, STATE Zip]

RE: Notice of Third Party Data Breach
Account Ending in: XXXX

Dear [Fname LName]:

Wescom Credit Union is writing to notify you of a recent incident involving a third-party service provider that may have affected the security of your personal information. We want to provide you with information about the incident, our response, and the steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened?

On May 14, 2019, an unauthorized party downloaded database backup files belonging to Geezeo, the provider for Wescom's eBudget services. Wescom was notified by Geezeo of this incident on or about September 24, 2019.

What Information Was Involved?

The impacted backup files contained historical Wescom member information dating from 2012, including name, address, account number, account type, account balance (as of 2012), email address, gender, birth year, and user and account information. The files may have also contained member's financial information from non-Wescom accounts (which varied by impacted member). The exposed data did not contain any Social Security numbers, passwords, security codes, access codes, or other similar information that would allow access to Wescom members' accounts.

What Are We Doing?

The security, privacy, and confidentiality of your personal information is among our highest priorities. Wescom has strict security procedures in place to verify our member's identity and account information before initiating transactions to protect our member's data.

Geezeo has also implemented additional security measures to prevent this from happening in the future. Wescom and Geezeo have notified the appropriate authorities and regulators to ensure the incident is properly addressed.

As an additional precaution, we are offering you access to 12 months of complimentary credit monitoring and identity theft restoration services through Equifax® at no cost to you. Details of this offer and instructions on how to enroll in the services are enclosed with this letter.

What You Can Do

We encourage you to closely monitor all of your financial accounts and immediately report any suspicious activity to the relevant financial institution. If you see anything you do not recognize on your Wescom account, please call Wescom right away. Also, we have enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information.

Additionally, you may sign up for free Account Alerts to monitor your Wescom accounts. Our selection of Account Alerts can help you keep track of your finances by notifying you via text message or email about activity on your account, loan(s), or Wescom cards.

For More Information

We apologize for any inconvenience this may cause you. If you have any questions, please call us at 1-888-4WESCOM (1-888-493-7266). You may also visit the Wescom Security Center at wescom.org/security to learn about online security, fraud, identity protection, and how to report fraud.

We remain committed to keeping your account and information safe and appreciate the trust you have placed in us as your financial service provider.

Sincerely,

Eli Martinez

Eli Martinez,
Vice President, Digital Channels

Steps You Can Take to Protect Your Information

ENROLL IN CREDIT MONITORING

As an added precaution, and at no cost to you paid by Geezeo, we have arranged to have Equifax protect your identity for 12 months. Below please find more information regarding the Equifax® **ID Patrol**® Credit Monitoring product, including how to enroll in the service.

Activation Code:

Enrollment Deadline: 2/1/2020

ONLINE ENROLLMENT INSTRUCTIONS

To sign up online go to www.myservices.equifax.com/patrol.

1. **Welcome Page:** Enter the Activation Code provided above in the "Activation Code" box and click the "Submit" button.
2. **Register**: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue" button.
4. **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

ADDITIONAL DETAILS REGARDING YOUR TWELVE MONTH EQUIFAX ID PATROL® CREDIT MONITORING PRODUCT:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- AutomaticFraud Alerts.[2] With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).

---

[1] Credit monitoring from Experian® and Transunion® will take several days to begin.

[2] The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

- Credit Report Lock[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning[4] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to $1 MM in identity theft insurance.[5]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

MONITOR YOUR ACCOUNTS/CREDIT REPORTS

We encourage you to remain vigilant against incidents of identity theft and fraud, review your account statements, and 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:

---

[3] Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4] Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[5] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

Experian	TransUnion	Equifax
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	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 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 member's credit file. Upon seeing a fraud alert display on a member'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	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.

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 has posted guidance pertaining to identity theft recovery at http://www.consumer.gov/idtheft. 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.