LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

September 3, 2020

VIA EMAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent Texell Credit Union ("Texell") in connection with a recent data security incident described in greater detail below. Texell is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On May 14, 2020, Texell discovered suspicious activity involving an employee's email account. In response to this discovery, we immediately changed the password for the employee's email account and began an investigation to determine what happened and whether information may have been accessed. On May 18, 2020, the investigation confirmed that an unauthorized individual had accessed the employee's email account but could not confirm whether personal information was accessed. We then engaged a data mining firm to conduct an extensive review of the contents of the impacted email account, and on July 7, 2020, we confirmed that the personal information of some of our members was contained in the email account that was accessed by the unauthorized individual. Please note, we are unaware of the misuse of any member information, and do not have evidence that personal information was actually accessed by the unauthorized individual. Member financial accounts were not accessed during this incident.

The information potentially impacted included members' names, addresses, account numbers, and Social Security numbers. While there is no evidence of the misuse of any personal information, out of an abundance of caution, Texell notified the potentially affected population.

2. Number of New Hampshire residents affected.

Texell notified four (4) New Hampshire residents regarding this data security incident. Notification letters were sent on September 3, 2020. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

Texell has taken steps in response to this incident to further strengthen the security of its email system in an effort to prevent similar incidents from occurring in the future. In addition, Texell has offered all affected individuals 12 months of credit monitoring and identity protection services at no charge to the individual.

4. Contact information.

Texell remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 Lindsay.Nickle@lewisbrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Consumer Notification Letter

<<Date>>

<<Name>>
<<Address>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
(833) 755-1018
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<,CODE>>

Re: Notice of Data Security Incident

Dear <<Name>> ,

I am writing to inform you of a data security incident that potentially involved your personal information. At Texell Credit Union ("Texell"), we take the privacy and security of our member information very seriously. This is why I am contacting you to share details about the incident, what we are doing to address it, steps you can take to help protect your information, and resources that we are making available to assist you.

What Happened? On May 14, 2020, Texell discovered suspicious activity involving an employee's email account. In response to this discovery, we immediately changed the password for the email account and launched an investigation. On May 18, 2020, the investigation confirmed that an unauthorized individual had accessed the employee's email account but could not confirm whether personal information was accessed. We then engaged a data mining firm to conduct an extensive review of the data in the affected email account. On July 7, 2020, we confirmed that your personal information was contained in the email account accessed without authorization. Please note, we are unaware of the misuse of any member information as a result of this incident.

What Information Was Involved? The information involved includes your name, address, Social Security number, and account numbers. No member financial accounts were accessed during this incident.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We have also taken steps to increase the security of the email accounts in our environment. In addition, we are offering you information about steps you can take to help protect your personal information. Out of an abundance of caution, we are also offering you free identity monitoring and identity recovery services for 12 months through ID Experts. These services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a United States residential address associated with your credit file. Please note that the deadline to enroll in the monitoring services is December 3, 2020.

What You Can Do: We recommend that you review the guidance included with this letter about how to help protect your information. You can also contact ID Experts with any questions and to

enroll in the free credit monitoring services by calling (833) 755-1018 or by going to https://app.myidcare.com/account-creation/protect.

We encourage you to take full advantage of this service offering. ID Experts representatives are fully versed on the incident and can answer questions or respond to concerns you may have.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call (833) 755-1018, Monday through Friday from 8:00 am – 8:00 pm Central Standard Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Amy Merriman
Chief Operating Officer
Texell Credit Union

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	401-274-4400
1-212-416-8433			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found above.