LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
429 4th Ave, Suite 805
Pittsburgh, Pennsylvania 15219
Lauren.Godfrey @lewisbrisbois.com
Direct: 412.567.5113

April 19, 2021

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

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Timber Creek, an FCS packaging Brand ("Timber Creek"), which is an industrial lumbar wholesaler and customer crating provider in Milwaukee, WI, in connection with a data security incident described in greater detail below. Timber Creek takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

On September 13, 2020, Timber Creek discovered that some of its computer systems had been encrypted. Timber Creek immediately took steps to contain the incident and secure its network systems. To that end, Timber Creek engaged a digital forensics firm to investigate the cause and scope of the incident and determine if any information stored within our systems had been affected. The forensic investigation determined that an unauthorized individual may have had access to certain files on its network. Timber creek then conducted a detailed and comprehensive review of the impacted information which concluded on February 10, 2021. We immediately worked to obtain addresses for the impacted individuals which concluded on March 28, 2021. The potentially affected information includes names, Social Security numbers, driver's licenses and financial account information.

2. Number of New Hampshire residents affected.

On April 15, 2021, Timber Creek issued notification letters to two (2) New Hampshire residents regarding this data security incident via first-class U.S. mail. A sample copy of the notification letter is attached hereto.

3. Steps taken relating to the incident.

Upon learning of this incident, Timber Creek took the steps described above. Timber Creek also updated its internal procedures and has implemented additional safeguards to help prevent a similar incident from occurring in the future including but not limited to increasing its password complexity requirements.

Timber Creek is also offering the potentially affected individuals 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services at no cost through IDX, to ensure their information is protected.

4. Contact information.

Timber Creek remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (412) 567-5113 or via email at Lauren.Godfrey@lewisbrisbois.com.

Very truly yours,

Lauren Godfrey

Lauren D. Godfrey, CIPP/US on behalf of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LDG
Encl. Consumer Notification Letter

TIMBERCREEK
AN FCA PACKAGING BRAND

C/O IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-664-1376
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: ##########

<<Full Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 15, 2021

Re: Notice of Data Security Incident

Dear <<Full Name>>,

Timber Creek ("Timber Creek") is writing to inform you of an incident that may have involved your personal information. We take the privacy and security of the information in our possession very seriously. Therefore, we are writing to inform you of the incident, and advise you of certain steps you can take to help protect your personal information, including activating the credit and identity monitoring services we are offering at no cost to you.

What Happened? On September 13, 2020, we discovered that some of our systems had been encrypted. Our immediate concern was to contain the incident and secure our network systems. To that end, we engaged a digital forensics firm to investigate the cause and scope of the incident and determine if any information stored within our systems had been affected. The forensic investigation determined that an unauthorized individual may have had access to certain files on our network. We then conducted a detailed and comprehensive review of the impacted information which concluded on February 10, 2021. That review determined that your personal information was involved in the incident. We immediately worked to obtain addresses for the impacted individuals, and to notify you of the incident.

We have no information to suggest that your information has been misused in any way. However, out of an abundance of caution, we are notifying you of the incident, and providing you with information about how to protect your personal information.

What Information Was Involved? The files that may have been accessed by the unauthorized individual include: <<variable data>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We have also reported the incident to the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to help prevent fraudulent activity and facilitate prosecution of the perpetrators. In addition, we have secured the services of IDX to provide identity monitoring at no cost to you for <<membership length>>. IDX is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your credit and identity monitoring services include: <<membership length>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

Please note you must enroll by July 15, 2021. If you have questions or need assistance, please call IDX at 1-833-664-1376.

What You Can Do: Please review the enclosed "Additional Resources" section included with this letter. It describes additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to activate the complimentary identity monitoring services we are making available through IDX.

For More Information: If you have questions or need assistance, please call 1-833-664-1376, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Standard Time. Please have your enrollment code ready.

Protecting your information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Steve Everett, Jr.

Steve Everett, Jr.
President
Timber Creek, an FCA Packaging Brand

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 by reviewing 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 also should 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 (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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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 and 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 **Bureau of Internet and Technology Resources**	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
28 Liberty Street	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
New York, NY 10005	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
ifraud@ag.ny.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
1-212-416-8433	1-888-743-0023	1-877-566-7226	401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

TIMBERCREEK
AN FCA PACKAGING BRAND

C/O IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-664-1376
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: ##########

<<Full Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 15, 2021

Re: Notice of Data Security Incident

Dear <<Full Name>>,

Timber Creek ("Timber Creek") is writing to inform you of an incident that may have involved your personal information. We take the privacy and security of the information in our possession very seriously. Therefore, we are writing to inform you of the incident, and advise you of certain steps you can take to help protect your personal information, including activating the credit and identity monitoring services we are offering at no cost to you.

What Happened? On September 13, 2020, we discovered that some of our systems had been encrypted. Our immediate concern was to contain the incident and secure our network systems. To that end, we engaged a digital forensics firm to investigate the cause and scope of the incident and determine if any information stored within our systems had been affected. The forensic investigation determined that an unauthorized individual may have had access to certain files on our network. We then conducted a detailed and comprehensive review of the impacted information which concluded on February 10, 2021. That review determined that your personal information was involved in the incident. We immediately worked to obtain addresses for the impacted individuals, and to notify you of the incident.

We have no information to suggest that your information has been misused in any way. However, out of an abundance of caution, we are notifying you of the incident, and providing you with information about how to protect your personal information.

What Information Was Involved? The files that may have been accessed by the unauthorized individual include your name and <<variable data>>. Your Social Security number was not involved in the incident.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We have also reported the incident to the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to help prevent fraudulent activity and facilitate prosecution of the perpetrators. In addition, we have secured the services of IDX to provide identity monitoring at no cost to you for <<membership length>>. IDX is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your credit and identity monitoring services include: <<membership length>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

Please note you must enroll by July 15, 2021. If you have questions or need assistance, please call IDX at 1-833-664-1376.

What You Can Do: Please review the enclosed "Additional Resources" section included with this letter. It describes additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to activate the complimentary identity monitoring services we are making available through IDX.

For More Information: If you have questions or need assistance, please call 1-833-664-1376, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Standard Time. Please have your membership number ready.

Protecting your information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Steve Everett, Jr

Steve Everett, Jr.
President
Timber Creek, an FCA Packaging Brand

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 by reviewing 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 also should 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 (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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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 and 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	www.oag.state.md.us	www.ncdoj.gov	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 to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.