



LEWIS BRISBOIS BISGAARD & SMITH LLP

Robert L. Slaughter III
633 W. 5th Street, Suite 4000
Los Angeles, CA 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

December 18, 2020

VIA E-MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Capital Lumber Company (“Capital”), a distributor of specialty building materials headquartered in Phoenix, Arizona. This letter is being sent because the personal information of one New Hampshire resident may have been affected by a recent data security incident experienced by Capital. The incident may have involved unauthorized access to one resident’s name and Social Security number.

On September 5, 2020, Capital detected a data security incident that disrupted access to certain systems. Upon discovering this, Capital immediately initiated an investigation and took steps to secure its network. This investigation involved the assistance of cybersecurity experts to determine whether sensitive information may have been accessed during the incident. The Federal Bureau of Investigation was also notified. As result of this investigation, Capital learned that personal information stored on certain systems and Capital email accounts may have been accessed during the incident between approximately July 27 and September 6, 2020. On or about November 13, 2020, Capital identified that personal information belonging to one New Hampshire resident may have been affected. Capital then worked diligently to provide notification as quickly as possible.

Capital notified one (1) potentially affected New Hampshire resident of this incident via the attached sample letter, or a substantially similar version, on December 18, 2020. In so doing, Capital offered one year of complimentary identity monitoring and identity theft restoration services through IDX, a global leader in risk mitigation and response. Please contact me should you have any questions.

Sincerely,

/s/ Robert Slaughter III

Robert Slaughter III of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

CAPITAL

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

To Enroll, Please Call:

833-920-3178

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXXXX>>

December 18, 2020

Re: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a recent data security incident that may have involved your personal information. At Capital Lumber Company (“Capital”), we are committed to the security of all information within our possession. This is why we are writing to notify you of this incident, to offer you complimentary identity monitoring services, and to inform you about steps that can be taken to help safeguard your personal information.

What Happened? On September 5, 2020, Capital experienced a data security incident that disrupted access to certain systems. Upon discovering this, we immediately took steps to secure our network and launched an investigation with the assistance of cybersecurity experts to determine what happened and whether sensitive information may have been accessed or acquired. The investigation revealed that personal information stored on certain systems and Capital email accounts may have been accessed or acquired between approximately July 27 and September 6, 2020. On November 13, 2020 following a thorough review, we identified your information as potentially involved. We then worked diligently to identify up-to-date address information to notify you.

What Information Was Involved? The information may have involved your <<insert variable text>>.

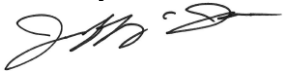
What We Are Doing. As soon as we discovered this incident, we took the measures referenced above and implemented enhanced security measures to help prevent a similar incident from occurring in the future. We have also notified the Federal Bureau of Investigation and will fully cooperate with any investigation. In addition, we are providing you information about steps you can take to protect your personal information and identity theft protection services through IDX, a data security and recovery services expert. Your complimentary one-year enrollment in IDX™ includes: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information. You can also enroll in the IDX services being provided to you, at no cost, through IDX. To enroll, please visit the IDX website at <https://app.idx.us/account-creation/protect> and provide your enrollment code located at the top of this page. Please note that the deadline to enroll is March 18, 2021. Additional information describing the IDX services, along with other recommendations to protect your personal information, is included with this letter.

For More Information. Please accept our sincere apologies for any worry or inconvenience that this may cause you. If you have any questions, please call 833-920-3178 Monday through Friday from 9 am to 9 pm Eastern Time, or please visit the

IDX website at <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. Please have your enrollment code ready.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeff Jenkins", with a long horizontal flourish extending to the right.

Jeff Jenkins
Vice President of Finance
Capital Lumber Company

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 also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400
---	--	--	--

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 other rights. 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.



One-Year Enrollment in IDX™

Website and Enrollment. Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 833-920-3178 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.