McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

RECEIVED
NOV 04 2022
CONSUMER PROTECTION

October 31, 2022

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Wm. T. Burnett – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Wm. T. Burnett & Co. and STX, LLC ("Wm. T. Burnett"). I am writing to provide notification of an incident at Wm. T. Burnett that may affect the security of personal information of approximately one (1) New Hampshire resident. Wm. T. Burnett's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Wm. T. Burnett does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On September 30, 2022, Wm. T. Burnett experienced unauthorized access to its network that involved ransomware. Upon learning of this issue, Wm. T. Burnett immediately commenced a prompt and thorough investigation. As part of its investigation, Wm. T. Burnett has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, Wm. T. Burnett discovered on October 6, 2022 that certain impacted files may have been removed from the network by an unauthorized individual(s). The files contained personal information of a New Hampshire resident including name, SSN, and financial account information associated with direct deposit.

Wm. T. Burnett is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Wm. T. Burnett wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Wm. T. Burnett is providing the affected resident with written notification of this incident commencing on or about October 26, 2022 in substantially the same form as the letter attached hereto. Wm. T. Burnett is offering the affected resident complimentary one-year membership with a credit monitoring service. Wm. T. Burnett will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Wm. T. Burnett will advise the affected resident

about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Wm. T. Burnett, protecting the privacy of personal information is a top priority. Wm. T. Burnett is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Wm. T. Burnett continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com.

Sincerely,

Christine N. Czuprynski

Encl.

Wm. T. Burnett & Co.
Return Mail Processed By:
IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

Wm. T. Burnett & Co.

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [redacted]

[redacted]

[redacted]

Re: Burnett Security Incident

Dear [redacted]:

We are writing to inform you of a recent security incident affecting a portion of our stored electronic data. That data may have included your personal information, the privacy and security of which are of the utmost importance to the Company, whether you are or were affiliated with Wm. T. Burnett & Co. and STX, LLC ("Company"). We wanted to provide you with information about the incident, explain the services we have made available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

The Company recently experienced a cybersecurity incident involving ransomware. Upon learning of this issue, we quickly contained the threat by disabling all unauthorized access to the network and immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the information on our network. Though our investigation is still ongoing, we concluded on or about October 6, 2022 that your personal information may have been accessed or acquired in connection with this incident.

What Information Was Involved?

The potentially acquired information included your personal information, specifically your [redacted]. The impacted information could also have included your [redacted].

What You Can Do.

To date, we are not aware of any misuse of your information as a result of this incident. Out of an abundance of caution, however, we want to advise you on the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection 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, IDX will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We apologize for the inconvenience caused by this attack, which occurred despite our focused efforts to combat this criminal behavior. We remain committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. In response to this incident, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts, including resetting account passwords and strengthening our password security policies, ensuring compliance with multi-factor authentication for network access, upgrading our firewall, and deploying endpoint detection software.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions. Please call [redacted] or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Sincerely,

Wm. T. Burnett & Co.
1500 Bush Street
Baltimore, MD 21230

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **IDX website** to enroll: **https://app.idx.us/account-creation/protect**
3. PROVIDE the **Enrollment Code Above**

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	*Experian*	*TransUnion LLC*
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	P.O. Box 6790 Fullerton, PA 92834-6790 https://www.transunion.com/fraud-alerts (800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any

accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.