CONSTANGY BROOKS, SMITH & PROPHETE LLP

February 6, 2024

<u>VIA EMAIL</u>
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: <u>Notice of Third-Party Data Security Incident</u>

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents McNeill Baur PLLC ("McNeill Baur") in connection with a recent data security incident described below.

1. What Happened

On November 30, 2023, McNeill Baur learned that one of its third-party vendors, Paycor, had experienced a data security incident arising from the MOVEit software vulnerability. The incident resulted in files pertaining to McNeill Baur being downloaded by an unauthorized actor on or around May 31, 2023. The incident was limited to the Paycor's systems, and no McNeill Baur networks or systems were affected. Based on information provided by Paycor, it was determined that the impacted files contained for some of McNeill Baur's current and former employees. McNeill Baur is not aware of any evidence that this information has been misused.

2. Number of New Hampshire Residents Notified

On December 22, 2023, McNeill Baur notified one (1) New Hampshire resident of this incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the potentially impacted individual is included with this correspondence.

3. Steps Taken Relating to the Incident

McNeill Baur understands that Paycor reported the incident to law enforcement and implemented technical measures to fix the MOVEit vulnerability shortly after it was publicized. Further, McNeill Baur is partnering with Experian to provide access to complimentary identity monitoring services to notified individuals. Those services include of credit and dark web monitoring, a $1 million identity theft insurance coverage, and fully managed identity restoration services.

4. Contact Information

McNeill Baur 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
or .

Best regards,

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

MB MCNEILL | BAUR
Intellectual Property Law

December 22, 2023

[redacted]

Subject: Notice of Data Security Incident

Dear :

We are writing to notify you about a cybersecurity incident experienced by our payroll vendor, Paycor, which may have affected your personal information. McNeill Baur PLLC ("McNeill Baur") takes this matter extremely seriously. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened: On November 30, 2023 Paycor notified us that it was one of many organizations across the globe that were recently affected by the MOVEit software vulnerability, and the incident resulted in some McNeill Baur files being downloaded by an unauthorized actor on May 31, 2023. Paycor utilizes the MOVEit tool to transfer data to and from its clients, including McNeill Baur. Paycor enlisted third-party experts to review and analyze certain Paycor servers, logs and devices that were potentially exposed to the unauthorized access. Paycor informed us that, based on its review, the impacted files contained personal information for some of McNeill Baur's current and former employees. Paycor provided us with a list of those individuals, and we took immediate steps to issue notification letters as quickly as possible.

What Information Was Involved: The information involved may have included your . Please note that we have no evidence of any actual or suspected misuse of this information.

What We Are Doing: Paycor retained a leading cybersecurity firm to conduct a forensic investigation into the incident, which confirmed that there was no evidence of compromise beyond the MOVEit transfer platform. Further, none of McNeill Baur's systems were affected. Paycor also reported the incident to law enforcement and implemented technical measures to fix the MOVEit vulnerability shortly after it was publicized. For McNeill Baur's part, we are reviewing relationships with each of our vendors to ensure that they are maintaining the necessary security standards and procedures to reduce the chances of a similar incident occurring again.

While we have no evidence that any of your information was misused, out of an abundance of caution we are offering you complimentary identity protection services through Experian—a data breach and recovery services expert. Experian IdentityWorks℠ services include of credit[1] and dark web monitoring, a $1 million identity theft insurance coverage, and fully managed identity restoration services in the event you become a victim of identity theft.

To start monitoring your personal information, please enroll by visiting https://www.experianidworks.com/credit or calling Experian's customer care team at 1-877-890-9332 and entering your unique Activation Code: . You will be asked to register an account and follow an identity verification process. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian. Please note that the deadline to enroll is (your code will not work after this date).

What You Can Do: We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, Experian can help you resolve issues if your identity is compromised. Please also review the guidance included with this letter which contains additional resources you may utilize to help protect your information.

McNeill Baur is taking this matter extremely seriously and deeply regrets any worry or inconvenience that this may cause. If you have any questions, please contact at

Sincerely,

Susan L. Statz
Operations Manager
McNeill Baur PLLC
125 Cambridge Park Drive, Suite 301
Cambridge, MA 02140

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE TO HELP 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 1-877-322-8228, 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:

Equifax	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.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 one year. 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 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.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	**Washington D.C. Attorney General** 441 4th Street, NW Washington, DC 20001 oag.dc.gov 1-202-727-3400	**New York Attorney General** Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 1-212-416-8433
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	**Maryland Attorney General** 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023

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 https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting- act.pdf.