MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 18, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Taft Stettinius & Hollister LLP ("Taft") located at 425 Walnut Street, Suite 1800 Cincinnati, Ohio, 45202 and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Taft does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 20, 2023, Taft discovered it was impacted by ransomware. As part of its incident response policies and procedures, Taft quickly identified the event involved unauthorized access to certain firm systems and data and took immediate steps to terminate the unauthorized access and mitigate any resulting harms. Taft worked extensively with several third-party security and forensics specialists to mitigate the impact of the incident and conduct a thorough forensic investigation to determine its root causes and the scope of the unauthorized access.

The investigation revealed unauthorized access to certain data stored on a limited number of secondary servers and workstations, some of which stored client and personal information. Taft began a comprehensive review of all of the files on the servers and workstations to determine if any individuals were affected. As required, Taft commenced notifying impacted clients, in accordance with its existing engagement letters and ethical requirements. On February 23, 2024,

Taft obtained initial address information for the first set of potentially affected individuals. Taft completed notice to these individuals on March 11, 2024. No New Hampshire residents were provided notice on this date. Simultaneously, Taft continued its' work to gather address information for individuals who may have been impacted. Taft completed this work on April 3, 2024.

The personal information that could have been subject to unauthorized access includes
.

Notice to New Hampshire Residents

On April 18, 2024, Taft began providing written notice of this incident to two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Taft moved quickly to investigate and respond to the incident, assess the security of Taft systems, and identify potentially affected individuals. Further, Taft notified federal law enforcement regarding the event. Taft has already implemented several changes to its information security practices and is also working to implement additional safeguards and improvements to its existing employee training and awareness efforts. Taft is providing access to credit monitoring services for , through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Taft is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Taft is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Taft is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/scs
Enclosure

EXHIBIT A

Taft/

Return Mail Processing
PO Box 999
Suwanee, GA 30024

25 1 5339 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

April 18, 2024

RE: [Extra1]

Dear Sample A. Sample:

Taft Stettinius & Hollister LLP ("Taft") writes to notify you of an incident that may have resulted in unauthorized access to your personal information. Taft, including the law firm of Chester Willcox, which was previously acquired by Taft, was in possession of your personal information in its archived files in connection with prior firm-related matters or firm business. As an individual, you may have been a Taft client or party related to a Taft client in one or more closed matters. For example, you may have been employed by a Taft client, a party that was related to a Taft client, or a party to a Taft client's matter. Once aware of the incident, Taft immediately took steps to eliminate the threat of further unauthorized access, safeguarded the information in its possession, and conducted a thorough forensic investigation and extensive data analysis to determine the scope of the incident. This letter is provided to you out of an abundance of caution, as well as to provide you with information about the incident and what you can do to remain vigilant in protecting your personal information.

What Happened?

On October 20, 2023, Taft discovered it was impacted by ransomware. As part of its incident response policies and procedures, Taft quickly identified that the event involved unauthorized access to certain secondary firm systems and data. Taft took immediate steps to terminate the unauthorized access and mitigate any resulting harms. Taft worked extensively with several third-party security and forensics specialists to mitigate the impact of the incident and conduct a thorough forensic investigation to determine its root causes and the scope of the unauthorized access.

The investigation revealed access to certain data stored in files on a limited number of servers and workstations between October 17, 2023 and October 20, 2023, some of which contained personal information. Please note that the incident **did not** impact Taft's primary firm systems such as Taft's document management system, email and other communications systems, or financial systems.

Please rest assured that Taft has taken all reasonable efforts to ensure the deletion of any misappropriated data from these files. To date, Taft has received no reports of further misuse of any of these files, to include the misuse of anyone's personal information.

What Information Was Involved?

While Taft's investigation has determined that only a fraction of the files in the affected servers and workstations were placed at risk, your personal information was maintained in archived files from firm business or for closed matters of the firm, and access to such information was possible as a result of the incident.

This personal information included: .
While it cannot be confirmed whether your personal information, specifically, was viewed or used by the unauthorized actor, Taft is providing notice to you so you can protect yourself, should you feel it is appropriate to do so.

What We Are Doing.

As part of its ongoing information security program, Taft has taken several steps to bolster its existing administrative and technical safeguards, improve its policies and procedures, and implement additional training to prevent the risk of a recurrence of an incident like this. Additionally, Taft continues to prioritize ongoing investment in its data governance and security infrastructure.

What You Can Do.

As previously stated, beyond the incident, Taft has not identified any misuse of the affected files or your personal information. However, we encourage you to always remain vigilant when it comes to monitoring your personal information. Please see Other Important Information below regarding additional steps you can take. ***Additionally, and to assist you with this vigilance, please see below where we have provided information on how to obtain of credit monitoring services and identity protection services from Experian at no cost to you.***

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact our call center at: 1-833-918-1326, which is available Monday through Friday, between the hours of 9 a.m. and 9 p.m. Eastern Time, excluding major U.S. holidays. Please be prepared to provide engagement number . You also may write to us at 425 Walnut Street, Suite 1800 Cincinnati, Ohio 45202-3957.

Sincerely,

Cathy Howard
General Counsel
Taft Stettinius & Hollister LLP

OTHER IMPORTANT INFORMATION

1. Complimentary Credit Monitoring and Identity Theft Services from Experian

Taft is providing complimentary credit monitoring services for , should you choose to enroll. To do so, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. 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. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/.

Equifax	***Experian***	***TransUnion***
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html 1-888-397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts 1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

The following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). 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/ 1-888-298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze 1-888-909-8872

In order to place the security freeze, you will 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.

For District of Columbia Residents: You may also contact the Attorney General for the District of Columbia for more information about how to protect your identity by using the information below: Attorney General's Office 400 6th Street, NW Washington, DC 20001 Phone: (202) 727-3400 Website: https://oag.dc.gov/	For Maryland Residents: You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 200 St. Paul Place Baltimore, MD 21202 Phone: 410-528-8662 Website: https://www.marylandattorneygeneral.gov/

For New York Residents: You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: 1-800-771-7755 Website: https://ag.ny.gov/	For North Carolina Residents: You may also contact the North Carolina Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Toll Free in NC: 1-877-566-7226 Outside NC: 919-716-6000 Website: https://ncdoj.gov/
For Oregon Residents: You can contact the Oregon Attorney General at: Oregon Department of Justice 1162 Court Street NE, Salem, OR 97301-4096, 1-877-877- 9392 www.doj.state.or.us.	For Rhode Island Residents: You may also contact the Rhode Island Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: 401-274-4400 Website: http://www.riag.ri.gov/ There is approximately 1 Rhode Island resident that may be impacted by this incident.