MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

February 2, 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 Info Tech, Inc. d/b/a Infotech ("Infotech") located at 2970 South West 50th Terrace, Gainesville, Florida 32608, and are writing to notify your office of an incident at an Infotech vendor that may affect the security of certain personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Infotech 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

Infotech formerly utilized Paycor HMN, Inc. ("Paycor") for human resources and payroll services. Paycor relies on a third-party software tool called MOVEit Transfer ("MOVEit"), developed by Progress Software, to send and receive certain data. On May 31, 2023, Progress Software announced that it had discovered a security vulnerability with the MOVEit software.

On December 29, 2023, Infotech was notified by Paycor that Paycor had completed a forensic investigation and determined that an unauthorized third party had exploited the MOVEit security vulnerability and obtained certain files. Following the investigation, Paycor then completed an extensive data analysis and determined that data related to certain current and former Infotech employees was affected and provided that list of impacted individuals to Infotech.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Resident

On or about February 2, 2024, Infotech provided written notice of this incident to one (1) New Hampshire resident. 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, Infotech moved quickly to validate the information identified by Paycor's data analysis and provide preliminary notice of the event to impacted individuals. Infotech is also reviewing their policies and procedures related to third-party vendor management. Infotech is also contacting Paycor to ensure any historical data within Paycor's possession is securely deleted in accordance with applicable laws. Infotech is also providing access to credit monitoring services for , through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Infotech is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Infotech 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. Infotech is providing written notice of this incident to relevant state regulators, as necessary.

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,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/jlm
Enclosure

EXHIBIT A

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Info Tech, Inc. d/b/a Infotech ("Infotech") writes as a follow up to the letter sent to your home on January 10, 2023 related to the event at Paycor that may affect the security of some of your information. **This is not a notice of a new event but is a supplement to the previous notification provided regarding this incident.** As discussed in further detail below, this incident did not involve or affect Infotech's network or IT systems. However, as we respect the privacy of your information, we wanted to provide you with information about this incident with a former vendor, as well as resources available to help you further protect your information, should you feel it necessary to do so.

What Happened?

Infotech formerly utilized Paycor HMN, Inc. ("Paycor") for human resources and payroll services. Paycor relies on a third-party software tool called MOVEit Transfer ("MOVEit"), developed by Progress Software, to send and receive certain data. On May 31, 2023, Progress Software announced that it had discovered a security vulnerability with the MOVEit software.

On December 29, 2023, Infotech was notified by Paycor that they had completed a forensic investigation and determined that an unauthorized third party had exploited the MOVEit security vulnerability and obtained certain files. Following the investigation, Paycor then completed an extensive data analysis and determined that some data related to current and former Infotech employees were affected, including your information.

What Information Was Involved?

Paycor's review of the data determined that your

What We Are Doing.

We take this event and the security of our employees' information very seriously. Upon being notified of the event, we moved quickly to validate the information identified by Paycor's data analysis and provide preliminary notice to those individuals impacted by the event. Further, Infotech is notifying appropriate regulators, as required. We are also providing you with information in the attached *Steps you Can Take to Help Further Protect Your Information* that you may use to help further protect your information, should you feel it necessary to do so. To reduce the risk of a similar event from occurring in the future, we are reviewing our policies and procedures related to third-party vendor management. Infotech is also contacting Paycor to ensure any historical data within their possession is securely deleted in accordance with applicable laws.

As an added precaution, we are providing you with access to of credit monitoring and identity protection services provided by Transunion. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Further Protect Your Information*. Please note that you must complete the enrollment process yourself, as we are not able to enroll you in these services on your behalf.

What You Can Do.

We encourage you to remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Further Protect Your Information*, which contains information on what you can do to further protect against possible misuse of your information. We also encourage you to enroll in the credit monitoring services being offered.

For More Information.

We understand you may have additional questions related to this event. For further information, please contact Christine Bonnell at .

Sincerely,

Carole Pickens
Vice President, Governance

STEPS YOU CAN TAKE TO HELP FURTHER PROTECT YOUR INFORMATION

Enroll in Monitoring Services

Credit Monitoring services will be provided by Cyberscout through Identity Force, a TransUnion company. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, these services include proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/infotech and follow the instructions provided. When prompted please provide the following unique code to receive services: [CODE] In order for you to receive these services, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.