

# **EXHIBIT 1**

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 Maine law, the applicability of the Maine 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 name, and Social Security number.

### **Notice to Maine Resident**

On or about January 10, 2024, Infotech provided written notice of this incident to one (1) Maine 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 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 twelve (12) months, 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.

# **EXHIBIT A**

[INDIVIDUAL NAME]  
[STREET ADDRESS]  
[CITY, STATE AND POSTAL CODE]  
[DATE]

## **NOTICE OF DATA BREACH**

Dear [INDIVIDUAL NAME]:

We respect the privacy of your information, which is why we are writing to let you know about a third-party data security incident that involves your personal information.

### **WHAT HAPPENED?**

Paycor, Infotech's former payroll service vendor, incorporated MOVEit Transfer into its service to send and receive certain data. On or about May 31, 2023, MOVEit's developer, Progress Software, announced that it had discovered a previously unknown "zero-day" cyber vulnerability in the MOVEit Transfer software. That same day, Paycor discovered it was affected by this security incident.

Paycor took steps including launching a forensic analysis with the assistance of outside experts to address its issue. Paycor's analysis confirmed the scope of its breach was limited to the third-party MOVEit Transfer platform. An unauthorized third party exploited the cyber vulnerability on the MOVEit Transfer platform to obtain certain files transferred through the software.

Paycor notified Infotech on **December 29, 2023** that Paycor completed an extensive data analysis and determined that some of Infotech's sensitive information was affected as a result of this incident.

### **WHAT INFORMATION WAS INVOLVED?**

To our knowledge, the data accessed included personal information such as Date of Birth and Social Security Number.

### **WHAT WE ARE DOING**

Infotech follows an established third-party vendor review process. As we continue to adhere to our processes, we will conduct a thorough review of existing policies and any controls otherwise to ensure our information is maintained securely.

Infotech confirmed that Paycor notified and is working with law enforcement to ensure the incident is properly addressed.


### **WHAT YOU CAN DO**

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

### **FOR MORE INFORMATION**

For further information and assistance, please contact Christine Bonnell.

Sincerely,

A handwritten signature in black ink that reads "Carole L. Pickens". The signature is written in a cursive, slightly slanted style.

Carole Pickens  
Vice President, Governance

## 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](http://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting [www.annualcreditreport.com](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 can access the printable request form at <https://www.annualcreditreport.com/manualRequestForm.action> or fill out the online form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax  
(866) 349-5191

[www.equifax.com](http://www.equifax.com)

P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742

[www.experian.com](http://www.experian.com)

P.O. Box 2002  
Allen, TX 75013

TransUnion  
(800) 888-4213

[www.transunion.com](http://www.transunion.com)

2 Baldwin Place  
P.O. Box 1000  
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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 [www.annualcreditreport.com](http://www.annualcreditreport.com).

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://consumer.ftc.gov/identity-theft-and-online-security>.

For more information, please visit [IdentityTheft.gov](https://IdentityTheft.gov) or call 1-877-ID-THEFT (877-438-4338). [A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, [is enclosed/can be found on the FTC's website at [https://www.bulkorder.ftc.gov/system/files/publications/501a\\_idt\\_a\\_recovery\\_plan\\_508.pdf](https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf)].]

### **OTHER IMPORTANT INFORMATION**

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.