January 12, 2024

[redacted]

Re: Notice of Data Breach

Dear [redacted],

We are writing to let you know about a data security incident that involved your personal information. We wanted to provide you with information about the event, our response, and steps you may wish to take to better protect against the possibility of identity theft and fraud.

What Happened? Back in April 2021 when Fidelity notified us that they would no longer be in the payroll processing business, Tax Technologies, Inc. ("TTI") entered into a transition agreement with Paycor, a payroll processing service company. As part of the implementation, employee data was uploaded to the Paycor systems directly from Fidelity. The implementation did not go as expected and TTI made the decision not to use Paycor and selected ADP as our new service provider effective January 2022. Paycor was informed of our decision and they provided confirmation that our account was terminated.

On December 18, 2023, Paycor notified us that our employees' information was compromised as a result of data breach that took place on or about May 31, 2023. Progress Software announced that it had discovered a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software, which was being utilized by Paycor. None of TTI's systems were involved in this incident.

What Information was Involved? Paycor notified us that the data accessed included your: full name, state of residence, date of birth and Social Security number.

What We Are Doing. TTI values your privacy and deeply regrets that this incident occurred. After receiving notification from Paycor, TTI conducted an investigation to determine the scope of the incident and to confirm that TTI's internal systems were not affected. TTI is also in the process of submitting a written demand to Paycor for further information related to the incident and for the removal of all TTI data from Paycor's, and Paycor's vendor's, systems. TTI is reviewing our existing policies and procedures and will be implementing additional security measures designed to help prevent the recurrence of such events and to better protect the privacy of TTI's valued employees in the future.

What You Can Do. We want to make sure our employees are protected against the risk of identity theft and the unauthorized use of their personal information. Please 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. If you are currently using a credit monitoring service, please keep a close eye on your credit report to identify fraudulent activities. If you do not use any credit monitoring, please notify us immediately so that we can offer you a service to use.

For More Information. Please reach out if you have any further questions. You may contact Paul Neumann at (704) 727-6936 between 7:00 a.m. - 4:00 p.m. EST, Monday through Friday.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Paul Neumann
HR Manager

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
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.

To file a complaint with the FTC, go to www.ftc.gov/idtheft 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.

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 or calling toll-free 877-322-8228. You can also 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	Experian	TransUnion
800-685-1111	**888-397-3742**	**800-916-8800**
www.equifax.com	**www.experian.com**	**www.transunion.com**
P.O. Box 740241	**535 Anton Blvd., Suite 100**	**P.O. Box 6790**
Atlanta, GA 30374	**Costa Mesa, CA 92626**	**Fullerton, CA 92834**

Security Freeze
You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without your express authorization. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554	**P.O. Box 2000**	**PO Box 105788**
Allen, TX 75013	**Chester, PA 19016**	**Atlanta, GA 30348-5788**
888-397-3742	**888-909-8872**	**800-685-1111**
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	**www.equifax.com/personal/credit-report-services**

In order to place a security freeze, you may be required to provide the consumer reporting agency with the following information:

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

Fraud Alert

You also have the right to place an initial or "extended" fraud alert on your file. An initial fraud alert is free and will stay on your credit file for a 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. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. To place a fraud alert on your credit report, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 2002	**P.O. Box 2000**	**PO Box 105069**
Allen, TX 75013	**Chester, PA 19016**	**Atlanta, GA 30348-5788**
888-397-3742	**800-680-7289**	**888-766-0008**
www.experian.com/fraud/center.html	**www.transunion.com/fraud-victim-resource/place-fraud-alert**	**www.equifax.com/personal/credit-report-services**

Police Reports

If you ever experience identity theft or fraud, you have the right to file a police report. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Additional Free Resources on Identity Theft

Federal Trade Commission. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

Internal Revenue Service ("IRS"). Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you

can take to address a fraudulent tax return filed in your name and what to do if you become a victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

For New York Residents. New York residents may wish to review the information on security breach response and identity theft protection provided by the following agencies:

New York Attorney General's Office Bureau of Internet and Technology 212-416-8433 https://ag.ny.gov/resources/individuals/consumer-issues/technology	**NYS Department of State's Division of Consumer Protection 800-687-1220 https://www.dos.ny.gov/consumerprotection**	**The New York State Department of Labor 888-469-7365 https://dol.ny.gov/report-fraud**

For North Carolina Residents. North Carolina residents may wish to review the information on how to prevent identify theft provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699-9001.