



James P. Miller
Attorney at Law
Jim.Miller@ofplaw.com
Direct: (703) 218-2154

September 4, 2023

VIA EMAIL ONLY

Maryland Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

**Re: Data Security Incident Notice
Pursuant to Md. Code Ann. Comm. Law § 14-3504**

Dear Sir or Madam:

In accordance with Maryland's Personal Information Protection Act, we are writing on behalf of our client, Einstein Technologies, Inc. ("ETI") (FEIN 45-4377328), to notify you of a data security incident potentially affecting the personal information of nine Maryland residents, who will receive a copy of the notification attached to this letter by U.S. mail and email.

On August 3, 2023, ETI learned from its outside human capital management (HCM) vendor, Paycor, Inc. (Paycor), that the MOVEit Transfer software Paycor uses to send and receive data was compromised. According to Paycor, on May 31, 2023, Progress Software Corporation announced it discovered a previously unknown "zero-day" cyber vulnerability in the MOVEit Transfer software used by various HCM providers. Paycor informed ETI that, on the same day, Paycor identified unusual activity on the MOVEit Transfer software and promptly took steps to address the issue. Additionally, Paycor indicated it launched a forensic analysis with the assistance of outside experts. Based on Paycor's reporting to ETI, Paycor's ongoing analysis indicates that some of ETI's sensitive information may have been affected because of the cyber vulnerability in the MOVEit Transfer software.

Although it is ETI's understanding that Paycor has yet to complete its analysis of ETI's company data, and that Paycor does not expect to send "final" notices until October 2023, ETI requested further details from Paycor to understand the scope of the data security incident and its impact on ETI's information, and that of its employees. Unfortunately, ETI is limited in what it knows about this event. According to Paycor, its own investigation is dependent, in part, upon the results of a third party evaluating the MOVEit Transfer software. In an effort to ensure any affected data was protected from further unauthorized access or acquisition, ETI asked Paycor whether it would provide credit monitoring services, but it has not agreed to do so at this point. ETI wishes to provide you with the foregoing information that it received from Paycor because the privacy of your personal information may be affected. ETI will endeavor to provide updates as soon as practicable when it receives further details from Paycor. However, at this time, ETI does not have

sufficient information from Paycor to confirm exactly which personal information may have been accessed as a result of the cyber vulnerability in the MOVEit Transfer software, including whether such information was in an encrypted or redacted state. Because Paycor serves as ETI's outside HCM vendor for payroll and related services, ETI believes the affected personal information could include, for example:

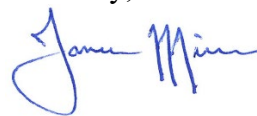
- Full name;
- Social security number;
- Birthdate;
- Phone number;
- A taxpayer identification number in combination with the income tax withheld for that taxpayer at the state and federal levels, including IRS Form W-2;
- A user name, email address, or any other account holder identifying information; and
- Financial account and routing numbers and related information, such as other data for direct deposits.

To be clear, ETI does not have confirmation that such personal information was the subject of unauthorized access or acquisition, including in an unencrypted or unredacted state, but ETI wants to apprise you of the types of information that could be involved in a data security incident such as the one ETI has been informed of by Paycor.

As set forth in the attached notification, ETI is advising the potentially affected Maryland residents of ETI's contact information, that of major consumer reporting agencies, the Federal Trade Commission, the Internal Revenue Service, the Office of the Attorney General, and further including a statement that an individual can obtain information from those sources regarding steps the individual can take to avoid identity theft, including by reporting attempted or actual identity theft and fraud to law enforcement.

Please feel free to contact me should you require additional information.

Sincerely,



James P. Miller

Attachment: A/S

cc: Einstein Technologies, Inc.
Thomas J. Sawyer, Esq.

Einstein Technologies, Inc.
901 North Monroe St.
Suite 914
Arlington, VA 22201
(703) 688-3243
www.einstein-tech.com

[DATE]

VIA U.S. MAIL AND EMAIL (Last Known Addresses)

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

Re: Data Security Incident

Dear [EMPLOYEE NAME]:

We value your service to Einstein Technologies, Inc. (ETI), and we respect the privacy of your personal information. As a precautionary measure, we are writing to inform you of a data security incident that may involve your personal information.

On August 3, 2023, ETI learned from its outside human capital management (HCM) vendor, Paycor, Inc. (Paycor), that the MOVEit Transfer software Paycor uses to send and receive data was compromised. According to Paycor, on May 31, 2023, Progress Software Corporation announced it discovered a previously unknown “zero-day” cyber vulnerability in the MOVEit Transfer software used by various HCM providers. Paycor informed ETI that, on the same day, Paycor identified unusual activity on the MOVEit Transfer software and promptly took steps to address the issue. Additionally, Paycor indicated it launched a forensic analysis with the assistance of outside experts. Based on Paycor’s reporting to ETI, Paycor’s ongoing analysis indicates that some of ETI’s sensitive information may have been affected because of the cyber vulnerability in the MOVEit Transfer software.

Although it is ETI’s understanding that Paycor has yet to complete its analysis of ETI’s company data, and that Paycor does not expect to send “final” notices until October 2023, ETI requested further details from Paycor to understand the scope of the data security incident and its impact on ETI’s information, and that of its employees. Unfortunately, we are limited in what we know about this event. According to Paycor, its own investigation is dependent, in part, upon the results of a third party evaluating the MOVEit Transfer software. In an effort to ensure any affected data was protected from further unauthorized access or acquisition, ETI asked Paycor whether it would provide credit monitoring services, but it has not agreed to do so at this point. ETI wishes to provide you with the foregoing information that it received from Paycor because the privacy of your personal information may be affected. ETI will endeavor to provide updates

as soon as practicable when it receives further details from Paycor. However, at this time, ETI does not have sufficient information from Paycor to confirm exactly which personal information may have been accessed as a result of the cyber vulnerability in the MOVEit Transfer software, including whether such information was in an encrypted or redacted state. Because Paycor serves as ETI's outside HCM vendor for payroll and related services, ETI believes the affected personal information could include, for example:

- Full name;
- Social security number;
- Birthdate;
- Phone number;
- A taxpayer identification number in combination with the income tax withheld for that taxpayer at the state and federal levels, including IRS Form W-2;
- A user name, email address, or any other account holder identifying information; and
- Financial account and routing numbers and related information, such as other data for direct deposits.

To be clear, ETI does not have confirmation that such personal information was the subject of unauthorized access or acquisition, including in an unencrypted or unredacted state, but ETI wants to apprise you of the types of information that could be involved in a data security incident such as the one ETI has been informed of by Paycor.

For further information, you may contact Martin B. Einstein at 703-688-3243. Also included below are resources about steps you can take to further protect your personal information and avoid identity theft.

In closing, we wish to reiterate ETI's respect and concern for the privacy of your personal information. We recognize this news may be unsettling, and we regret that your personal information may have been affected by the cyber vulnerability in the MOVEit Transfer software used by Paycor.

Very respectfully,

Marty Einstein
President and Engineer
Einstein Technologies, Inc.

Steps you can take to further protect your information and avoid identity theft:

Out of an abundance of caution, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. You can obtain information from the following sources, among others, about steps you can take to avoid identity theft. 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. The FTC's Headquarters address is 600 Pennsylvania Avenue, NW, Washington, DC 20580.

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 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 print a copy of the request form at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf>. Or you may 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 (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374
- Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626
- TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

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 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.

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).

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 may need to 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.

If you believe your email account may be affected, you should promptly change your username or password and security question or answer, as applicable, or to take other steps appropriate to protect the email account with the businesses and other online accounts for which you use the same username or email and password or security question or answer.

You may also wish to consult Internal Revenue Service resources about tax-related identity theft prevention, detection, and victim assistance: <https://www.irs.gov/identity-theft-fraud-scams>.

For Maryland Residents: You may contact the Maryland Office of the Attorney General toll free at 1-888-743-0023 (Baltimore Metro Area Office); 200 St. Paul Place, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov/>.

For New Jersey Residents: You may contact the Cyber Crimes Unit of the New Jersey State Police, a Division of the New Jersey Attorney General's Office, at (609) 584-5051 ext. 5664; New Jersey State Police, P.O. Box 7068, West Trenton, NJ 08628; <https://nj.gov/njsp/division/investigations/cyber-crimes.shtml>.

For Virginia Residents: You may contact the Computer Crime Section of the Virginia Attorney General's Office at (804) 786-2071 (Monday-Friday, 8:30 a.m.-5 p.m. ET); Computer Crime Section, Virginia Attorney General's Office, 202 North 9th Street, Richmond, VA 23219; <https://www.oag.state.va.us/ccsweb2/index.php>.