



Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Benjamin D. Wanger
direct dial: 215.564.1601
bwanger@bakerlaw.com

June 24, 2022

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, New Tech Solutions, Inc. (“New Tech”), to notify you of a data security incident involving a Maryland resident.

New Tech recently concluded an investigation into a security incident which impacted the availability and functionality of its corporate network. Upon discovering the incident, New Tech immediately took measures to contain the incident, notified law enforcement, and began an investigation. Through New Tech’s investigation, it determined that between May 2, 2022, and May 30, 2022, an unauthorized actor potentially accessed certain files contained on its network. New Tech conducted a thorough review of the files that were potentially accessed by the unauthorized actor and on June 14, 2022, determined that the files contained the name, Social Security number, and financial account number of one Maryland resident.

On June 24, 2022, New Tech mailed a notification letter via United States Postal Service First-Class mail to the individuals whose information may have been involved, including the one Maryland¹ resident, in accordance with Md. Code Ann., Com. Law § 14-3504. A copy of the notification letter is enclosed. New Tech is offering the Maryland resident a complimentary

¹ This report is not, and does not constitute, a waiver of New Tech’s objection that Maryland lacks personal jurisdiction over New Tech regarding any claims related to this data security incident.

June 24, 2022

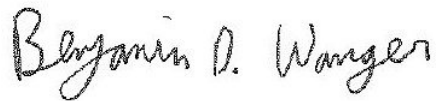
Page 2

membership to credit monitoring and identity protection services through IDX. New Tech also provided a phone number for individuals to call with any questions they may have.

To help prevent something like this from happening in the future, New Tech has implemented additional security measures to enhance the security of its network and is continuing to train its employees concerning data security.

Should you have any questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink that reads "Benjamin D. Wanger". The signature is written in a cursive, slightly slanted style.

Benjamin D. Wanger
Counsel

Enclosure



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code:

<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

June 24, 2022

Dear <<First Name>> <<Last Name>>:

New Tech Solutions, Inc. recognizes the importance of protecting the personal information we maintain. We are writing to let you know of a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some additional steps you may consider taking in response.

We recently detected a security incident which impacted the availability and functionality of our corporate network. Upon discovering the incident, we immediately took measures to contain the incident, notified law enforcement, and began an investigation. Through our investigation, we determined that between May 2, 2022, and May 30, 2022, an unauthorized actor potentially accessed certain files contained on our network. We conducted a thorough review of the files that were potentially accessed by the unauthorized actor and on June 14, 2022, we identified one or more file(s) containing your name, Social Security number, and the financial account number that you use for direct deposit.

We regret any inconvenience or concern this incident may cause you. We encourage you to remain vigilant by regularly reviewing your credit reports and financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact the relevant financial institution immediately. We are offering you one year of complimentary identity monitoring services through IDX. IDX identity protection services include: one year of tri bureau credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

We encourage you to contact IDX to enroll in the free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. Please note the deadline to enroll is **September 24, 2022**. For more information on identity theft prevention, please see the pages following this letter. IDX is open Monday through Friday, from 6:00 a.m. to 6:00 p.m., Pacific Time.

To help prevent a similar incident from occurring in the future, we have implemented additional security measures to enhance the security of our network and we are continuing to train our employees concerning data security. If you have any questions about the incident, please call me at 510-353-4070, Extension 312, Monday through Friday, from 9:00 a.m. to 5:00 p.m., Pacific Time.

Sincerely,

Vijay Kumar
CEO

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

New York residents may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

You can contact New Tech Solutions, Inc. via mail at 4179 Business Center Drive, Fremont, CA 94538, or via telephone at 510-353-4070.