

BakerHostetler

Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

December 8, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, TTEC Services Corporation (“TTEC”), to provide notice to your office concerning a security incident involving New Hampshire residents.¹ TTEC is located at 9197 South Peoria Street, Englewood, Colorado 80112.

On September 12, 2021, TTEC determined that certain devices in its network had been encrypted with ransomware. TTEC immediately activated its incident response and business continuity protocols, isolated the systems involved, and took other measures to contain the incident and to restore operations. TTEC launched an investigation, and a forensic firm that has assisted other companies in similar situations was engaged. Law enforcement was notified, and TTEC worked to support the investigation.

TTEC learned that there was unauthorized activity in TTEC’s network between March 31, 2021 and September 12, 2021. During that time, an unauthorized party obtained files stored on some of TTEC’s servers. TTEC completed a careful review of those files and other files on the servers on November 24, 2021 and determined that the files contained the names and Social Security numbers of 60 New Hampshire residents.

Beginning on December 8, 2021, TTEC will mail notification letters via First Class mail to the New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20. TTEC is providing individuals a complimentary, one-year membership to credit monitoring and identity theft protection

¹ This notice does not waive TTEC’s objection that New Hampshire lacks personal jurisdiction over it regarding any claims relating to this incident.

December 8, 2021

Page 2

services. TTEC has also established a dedicated, toll-free call center that individuals can call to obtain more information regarding the incident.

TTEC has taken a number of measures to address the incident. These measures include conducting network monitoring using the SentinelOne EDR tool, resetting passwords, and expanding multifactor authentication for remote access.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Joseph L. Bruemmer", with a long horizontal flourish extending to the right.

Joseph L. Bruemmer
Counsel

Enclosure



P.O. Box 989728
West Sacramento, CA 95798-9728

Credit Monitoring Enrollment
To Enroll, Please Visit:
<https://response.idx.us/dataservices>
Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: March 6, 2022

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<ADDRESS3>>
<<CITY>>, <<STATE>> <<ZIP>>
<<COUNTRY>>

December 8, 2021

Dear <<FIRST NAME>> <<LAST NAME>>,

TTEC understands the importance of protecting the information we hold, and the security of your information is a priority for us.

As TTEC previously disclosed, the company detected and addressed a cyber security incident in September 2021. In connection with the incident, a thorough investigation was performed, and we recently learned that the incident involved some of your information. This notice explains the incident, outlines the measures TTEC has taken in response, and provides some additional steps you can take to protect your information.

As soon as TTEC learned about the cyber security incident, we immediately began an investigation, and cyber security firms that have assisted other organizations with similar matters were engaged. We also notified law enforcement and have been supporting their investigation.

We learned that there was unauthorized activity in our network between March 31, 2021 and September 12, 2021. During that time, an unauthorized actor obtained files stored on some of our servers. We completed a careful review of those files and other files on the servers on November 24, 2021 and determined that one or more of the files contained your <<Variable Data>>.

As a precaution, we are offering you credit monitoring and identity protection services through the company IDX at no cost to you. These identity protection services include one year of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. These services are completely free to you, and enrolling in this program will not hurt your credit score. **For more information on the services, including instructions on how to activate your complimentary one-year membership, please visit <https://response.idx.us/dataservices> or call 1-833-325-1779 and use the Enrollment Code provided above. Please note the deadline to enroll is March 6, 2022.** For more information on identity protection and steps you can take in response, please see the additional information provided with this letter.

We regret that this incident occurred and apologize for any inconvenience. To help prevent something like this from happening again, we have taken steps to enhance our security measures. If you have additional questions, please call 1-833-325-1779, Monday through Friday, between 7:00 a.m. and 7:00 p.m., Mountain Time.

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.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

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.

TTEC is located at 9197 S. Peoria St., Englewood, Colorado and can be reached at 1(800) 835-3832.

Additional Information for Residents of the Following States:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You 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> | *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: 6 Rhode Island residents are receiving notice of this incident.>> Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

