

RECEIVED

JUL 29 2020

CONSUMER PROTECTION

BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

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

July 28, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing to notify you of a data security incident on behalf of my client, OTR Leasing, LLC, a buyer of late model used tractors, which they then lease and/or sell to owner-operators.

OTR Leasing recently concluded its investigation of a data security incident that involved unauthorized access to a limited number of employee email accounts. Upon suspecting potential unauthorized access to the employees' email accounts, OTR Leasing immediately secured the email accounts and launched an investigation, with the assistance of an outside cyber security firm.

As part of the investigation, OTR Leasing conducted a comprehensive review of the emails and attachments in the email accounts to identify individuals whose information may have been involved in this incident. Through the investigation, OTR Leasing determined that an unauthorized party accessed the employees' email accounts between the dates of January 14, 2020 and January 20, 2020. The investigation was unable to rule out the possibility that the unauthorized party may have been able to access emails and attachments in the accounts. In an abundance of caution, we reviewed the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person and on June 8, 2020, determined the name and one or more of: Social Security number and driver's license number of 28 New Hampshire residents were contained in the emails and attachments in the account.

On July 28, 2020, OTR Leasing will mail notification letters via United States Postal Service First-Class mail to the New Hampshire residents whose information may have been involved in this incident, in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is

July 28, 2020

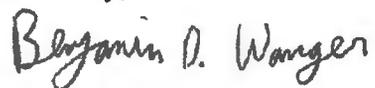
Page 2

enclosed. OTR Leasing is offering one year of complimentary credit monitoring and identity theft protection service through Kroll to the individuals whose Social Security number was in the accessed accounts. OTR Leasing has also established a dedicated call center where all individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, OTR Leasing has reset all employee passwords, limited external email access, continued to educate users on how to identify and avoid malicious emails, and added additional authentication measures for remote email access.

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

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



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

OTR Leasing understands the importance of protecting our customers' information. Regrettably, we are writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently learned that an unauthorized person gained access to a limited number of employee email accounts with personal information between January 14, 2020 and January 20, 2020. We immediately secured the accounts and a leading cyber security firm was hired to assist with the investigation. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts. In an abundance of caution, we reviewed the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person and on June 8, 2020, we determined that an email or attachment contained your <<b2b_text_1 (Impacted Data)>>.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. As a precaution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **October 27, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

We deeply regret any inconvenience or concern that this incident may cause. To help prevent something like this from happening again, we reset all employee passwords, limited external email access, continued to educate users on how to identify and avoid malicious emails, and added additional authentication measures for remote email access. To assist with any further questions or requests for information that you may have, we have set up a dedicated third-party call center. Please call 1-844-952-2233, Monday to Friday between 8:00 am and 5:30 pm Central Time.

Sincerely,

Patrick Meyer
Director of Finance

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.

Additional Information for Residents of the Following States:

Maryland: You may contact OTR Leasing at 9100 Liberty Dr, Pleasant Valley, MO 64068. 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>; and *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: This incident involves XX individuals in Rhode Island. 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

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.

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.