

BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501
T 215.568.3100
F 215.568.3439
www.bakerlaw.com

January 4, 2022

Anthony P. Valach
direct dial: 215.564.2588
avalach@bakerlaw.com

VIA E-MAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Ave.
Department 125
Bismarck, ND 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Central Specialties Inc. (“Central”), to notify your office of a cybersecurity incident. Central’s headquarters is located at 6325 County Rd 87, Alexandria, MN, 56308.

On August 23, 2021, Central became aware of a security incident that involved unauthorized access to some employee email accounts. Upon learning of the incident, Central promptly secured the accounts and a cybersecurity firm was engaged to assist. Through the investigation, we determined that an unauthorized actor may have accessed the employee email accounts between August 18, 2021 and August 23, 2021. Central completed a comprehensive review of the emails and attachments that could have been accessed and, on November 22, 2021, determined that an email or attachment contained the names, Social Security numbers, dates of birth, driver’s license numbers, financial account numbers, payment card numbers, and/or medical information of 301 North Dakota residents.

On January 4, 2022, Central will begin mailing notification letters to the North Dakota residents in accordance with N.D. Cent. Code § 51-30-01¹, via United States First-Class mail. A copy of the notification letter is enclosed. Central is offering the North Dakota residents a complimentary one-year subscription to identity monitoring services through Kroll. A dedicated, toll-free call center has been established for individuals to call with questions about the incident.

¹ This report does not waive Central’s objection that North Dakota lacks personal jurisdiction over it related to any claims that may arise from this incident.

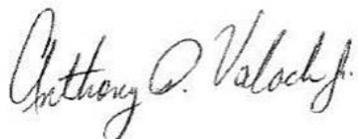
January 4, 2022

Page 2

To help prevent something like this from happening in the future, Central has implemented measures to enhance existing security and continues to educate its staff on how to identify and avoid malicious emails. Central has also established a dedicated call center to answer any questions residents may have about the incident.

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

Sincerely,

A handwritten signature in cursive script that reads "Anthony P. Valach".

Anthony P. Valach
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>>:

Central Specialties Inc. ("Central") understands the importance of protecting the information we maintain. We are writing to inform you of an incident that involves some of your personal information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

On August 23, 2021, Central became aware of a security incident that involved unauthorized access to some employee email accounts. Upon learning of the incident, Central promptly secured the accounts and a cybersecurity firm was engaged to assist. Through the investigation, we determined that an unauthorized actor may have accessed the employee email accounts between August 18, 2021 and August 23, 2021. Central conducted a comprehensive review of the emails and attachments that could have been accessed and, on November 22, 2021, determined that an email or attachment contained your <<b2b_text_1(DataElements)>>.

We wanted to notify you of the incident and assure you that we take it very seriously. As a precaution, we are offering you a complimentary one-year membership to Kroll Identity Monitoring services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. The credit and identity monitoring services are completely free to you and activating in this program will not hurt your credit score. **For more information about the credit and identity monitoring services, including instructions on how to activate your complimentary one-year membership, please visit: <https://enroll.krollmonitoring.com>. You have until <<b2b_text_6 (Activation Deadline)>> to activate your credit and identity monitoring services. Your Membership Number to enroll is: <<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

We regret any inconvenience or concern this incident may cause you. To help prevent something like this from happening in the future, we have implemented measures to enhance our existing security and continue to educate our staff on how to identify and avoid malicious emails. We have also established a dedicated call center to answer any questions you may have about the incident. For more information about the incident, please call 1-???-???-????, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time, excluding some U.S. holidays. Please have your membership number ready.

Sincerely,

Ross Larson, CPA
Chief Financial Officer



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holiday. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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.

You may contact Central Specialties Inc. via U.S. mail at 6325 Co Rd 87 SW, Alexandria, MN 56308 or via telephone at 320-762-7289.

Additional information for residents of the following states:

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

New Mexico: 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 NW, 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.