

STATE OF NH
DEPT OF JUSTICE
2021 FEB 18 AM 11:11

BakerHostetler

Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

February 15, 2021

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:

We are writing on behalf of our client, Cintas Corporation ("Cintas"), to notify your office of a security incident. Cintas's headquarters are located at 6800 Cintas Boulevard, Mason, Ohio 45040.

Cintas identified a security incident on September 20, 2020 that caused certain devices in its network to become unavailable. Cintas immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. Cintas also notified law enforcement and worked to support the investigation.

The investigation determined that there was unauthorized activity on Cintas's network between September 16, 2020 and September 20, 2020. During that time, there was unauthorized access to folders on Cintas's file servers. The investigation was not able to determine which files in these folders might have been accessed, so out of an abundance of caution, Cintas conducted a careful review of the folders to see what kinds of information they contained. Cintas completed the review on December 25, 2020 and determined that there were files that contained information about current and former partners. For the two New Hampshire residents whose information may have been involved, the files included the individuals' names and financial account numbers.

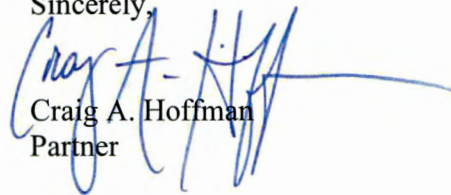
Attorney General Gordon MacDonald
Office of the Attorney General
February 15, 2021
Page 2

Beginning today, Cintas is mailing notification letters via U.S. mail to the New Hampshire residents.¹ A copy of the notification letter is attached. Cintas also has established a dedicated call center that individuals can call with questions about the incident.

To reduce the risk of a similar incident occurring in the future, Cintas has already implemented additional security measures to further enhance the security of its network, including an endpoint detection and response tool, a new managed security service provider, and enhanced alerting and response capabilities.

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

Sincerely,



Craig A. Hoffman
Partner

Enclosures

¹ This report does not waive Cintas's objection that New Hampshire lacks personal jurisdiction over Cintas regarding any claims related to this incident.

Cintas Corporation
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



[REDACTED]
[REDACTED]
[REDACTED]

H-48

February 12, 2021

Dear [REDACTED]:

Cintas Corporation understands the importance of protecting information. We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

We identified an incident on September 20, 2020 that caused certain devices in our network to become unavailable. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We also notified law enforcement and worked to support their investigation.

The investigation determined that there was unauthorized activity on our network between September 16, 2020 and September 20, 2020. During that time, there was unauthorized access to folders on our file servers. The investigation was not able to determine which files in these folders might have been accessed, so out of an abundance of caution, we conducted a careful review of the folders to see what kinds of information they contained. We completed the review on December 25, 2020 and determined that there were files that contained information about current and former partners. The information in the files included your name and financial account number ending in 3722.

Although we do not know whether files containing this information were actually accessed, we wanted to notify you of this incident and to assure you that we take it seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution. For more information on additional steps you can take, please see the additional information provided with this letter.

We regret that this occurred and apologize for any inconvenience. We have already implemented additional measures to further enhance the security of our network. If you have additional questions, please call 1-888-955-0999, Monday through Friday, between 8 a.m. and 5 p.m., Eastern Time.

Sincerely,

A handwritten signature in black ink that reads "Jennifer K. Mueller".

Jennifer Mueller
Vice President of Human Resources

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:

Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

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

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.