THOMPSON HINE

ATLANTA CINCINNATI COLUMBUS NEW YORK
CHICAGO CLEVELAND DAYTON WASHINGTON, D.C.

April 27, 2023

VIA FEDEX

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

RECEIVED
APR 28 2023
CONSUMER PROTECTION

Re: Cyber Incident Notification

Dear Attorney General Formella:

This communication serves as notice, on behalf of our client Dayton Superior Corporation ("DSC"), of a recent cybersecurity incident that affects New Hampshire residents.

As background, DSC is a manufacturing organization with its headquarters at 1125 Byers Road, Miamisburg, OH 45342. In February 2023, DSC identified unusual activity occurring within its information networks and systems and discovered that a third party had unauthorized access to the company's information technology environment. DSC immediately deployed security measures to contain and mitigate the threat and retained an external incident response team to accelerate recovery efforts. As part of its investigation into the incident, DSC discovered that personnel files and other "HR" data were compromised. This information relates to

On April 27, 2023, DSC began notifying all individuals whose personal data may have been affected by this incident, which **included one (1) New Hampshire resident**. The aforementioned notifications were in substantially the same form as the attached letter (See Enclosure). DSC's notification to New Hampshire residents was undertaken in compliance with the direct and substitute notice requirements set forth in N.H. Rev. Stat. § 359-C:19-20.

DSC has offered each impacted individual **complimentary, multi-year credit monitoring services** through Equifax. DSC has further established a dedicated call support line and website to answer any questions that impacted individuals may have about this incident.

DSC has proactively engaged the **Federal Bureau of Investigation** and is continuing to cooperate with its investigation.

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

Sincerely,

Steven G. Stransky, Partner
Thompson Hine LLP
127 Public Square # 3900
Cleveland, OH 44114

Enclosure: Data Incident Notification Letter (Example)

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notification of Data Breach

Dear <<Name 1>>,

Dayton Superior Corporation ("**DSC**" or the "**Company**") must regrettably inform you that we were recently the victim of a cyberattack and that your personal data may have been compromised during this incident. We understand that receiving this notice may cause you frustration, and we get it – we are frustrated too. In today's world, cyberattacks have become extremely sophisticated and are impacting organizations of all sizes and in all business sectors. We have proactively notified the Federal Bureau of Investigation (**FBI**) of this incident and hope that our law enforcement agencies can take action against the group responsible for this incident.

This letter will explain the scope of the incident, and the complimentary credit monitoring services that we are offering you. Fortunately, there is **no indication** that your personal data has been misused, and we have taken measures to better ensure it will not be misused in the future.

However, out of an abundance of caution, we are offering credit monitoring services to our employees and their immediate family members. If you or your family members are already enrolled in credit monitoring services through DSC, then we will **automatically extend** these services by an additional three (3) years for a total of five (5) years of protection. If you have not enrolled in DSC's previous offers for such services, we encourage you to do so now and **new enrollees** will be eligible to receive five (5) years of credit monitoring services.

What Happened

In February 2023, our internal security monitoring tools identified that certain databases and files within our information technology (IT) networks and systems were being encrypted as part of a cyberattack. Prior to this incident, we purchased and implemented several IT security tools, which enabled us to quickly identify and remediate the incident. In fact, DSC was almost fully operational within 72 hours of the attack. However, out of an abundance of caution, we retained an IT consultant to independently investigate the incident and provide an assessment of our cybersecurity program.

In March 2023 - approximately five (5) weeks after the incident first occurred - the group responsible for the attack contacted DSC and indicated that they had stolen Company data, which included proprietary data and personal data related to our employees. In response, we engaged the FBI in the hopes they would investigate this matter and bring these criminals to justice.

In addition, with the assistance of security consultants, we directly engaged with the group responsible for this cyberattack. Based on the measures that we have implemented and the actions we have taken, there is **no indication** that your personal data has been misused or will be misused in the future.

What Information Was Involved

As noted above, the group that was responsible for this attack was able to gain access to Company data, including t
. We retained this personal data to comply with our own legal obligations (e.g., tax filings, employment eligibility) and to facilitate employee support functions, like l
. This type of personal data included ;

What We Are Doing

We understand the importance of having a comprehensive information security program, and we have taken action to remediate this cybersecurity incident and help prevent future occurrences. For instance, we have been undertaking, either alone or in conjunction with our IT consultants, the following: analyzing our end-point monitoring tools, firewalls, and authentication process to ensure they properly align with our business expectations; assessing our access and user-credential policies and protocols; and, reviewing our IT security and vulnerability testing programs. In addition to notifying the FBI, we are in the process of filing reports with applicable state regulatory authorities regarding the nature and scope of this cybersecurity incident.

Credit Monitoring Services / What You Can Do

To help address any concerns you may have, DSC will provide you, and your immediate family members, with complimentary credit monitoring services. If you or your family members are already enrolled in credit monitoring services through DSC, then we will automatically extend these services by an additional three (3) years in order to provide you a total of five (5) years of protection. If you have not enrolled in DSC's previous offers for such services, we encourage you to do so now and new enrollees will be eligible to receive five (5) years of credit monitoring services. The enclosed sheet provides instructions for how you can enroll to receive the **Equifax Credit Watch™ Gold** and **Equifax Child Monitoring Package** services, and other measures you can take to better protect yourself.

Point of Contact

We have established a dedicated call center to answer questions you may have about this incident, which you can reach at
4 from Monday – Friday, 9:00 am to 9:00 pm Eastern. We have also established a website about this incident, and it is available at .

Please know that we will stay committed to protecting your trust in us and we continue to be thankful and grateful for your support.

Sincerely,

Mark D. Carpenter
President & Chief Executive Officer

Additional Information

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 data 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.

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, North Carolina, Oregon, or Rhode Island, you may contact and obtain information from your state Attorney General at the following:

- California Department of Justice, Office of Privacy Protection, PO Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, www.oag.ca.gov/privacy.
- Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, www.ct.gov/ag, 1-860-808-5318.
- Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-515-281-5164, http://www.iowaattorneygeneral.gov/.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300.
- Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, www.mass.gov/ago/contact-us.html, 1-617-727-8400.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.
- Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-503-378-4400, http://www.doj.state.or.us.
- Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

If you are a resident of Massachusetts or Rhode Island, please note that pursuant to Massachusetts or 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.

If you are a resident of 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 below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies (see below).

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. 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:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (the "FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Federal Trade Commission has published a list of the primary rights created by the FCRA, and the article is available at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, and that article refers individuals seeking more information to visit www.ftc.gov/credit. The Federal Trade Commission's list of FCRA rights includes the following:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including

identity theft.

- 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 receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.

****

EQUIFAX®

<<Name 1>>
Enter your Activation Code: <<Enrollment Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal data, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to *www.equifax.com/activate*
Enter your unique Activation Code of <<Enrollment Code>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal data is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal data is at risk of being traded. [2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

EQUIFAX®

Enter your Activation Code: <<Enrollment Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Child Monitoring Package *(for Equifax Credit Watch™ Gold members)*

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications of activity on the child's Equifax credit report

Enrollment Instructions

Parent/guardian, after completing your enrollment in Equifax Credit Watch™ Gold:

Return to *www.equifax.com/activate*

Enter your unique Activation Code of <<Enrollment Code>> for Equifax Child Monitoring Package then click "Submit" and follow these additional steps.

1. **Sign In:**
   Click the 'Sign in here' link under the "Let's get started" header.
   Sign in with your email address and password you created when initially creating your account.
2. **Checkout:**
   Click 'Sign Me Up' to finish your enrollment.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package

You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child"
3. From there, enter your child's first name, last name, date of birth and social security number.
   Repeat steps for each minor child (up to four)

Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.