Appendix 1
Mativ US (non-Massachusetts – Credit Watch Gold) Letter Template

<Return Name>
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<Address3>
<City><State><Zip>

<<Date>>

Subject: Notice of Data Incident

Dear <<First Name>>,

We are writing to share with you important information regarding a data incident that potentially involved your personal information. We take this incident very seriously and are providing you with information, as well as access to resources, so that you can better protect your personal information and diligently monitor your accounts.

What Happened:

Through recent investigations, it has become apparent that for a period of time during June and July of this year, an unauthorized person blocked our access to parts of our network and systems and may have gained access to the personal information of certain employees of the legacy Schweitzer-Mauduit International, Inc. ("SWM") and Scapa Group, Ltd. ("Scapa") companies within the Mativ Holdings, Inc. group. We immediately disconnected the legacy SWM and Scapa IT networks from the internet, and a third-party security firm was engaged to assist with an investigation into the incident.

What Information was Involved:

The investigation was unable to determine what personal information, if any, the unauthorized person actually viewed. In an abundance of caution, we reviewed the data potentially accessed by an unauthorized person and, on August 12, 2022, determined that the unauthorized person may have accessed certain personal information, which may have included the following: date of birth, limited medical information, financial account number, and Social Security number.

What We are Doing:

Immediately upon learning of the incident, we took steps to ensure that the unauthorized person no longer had access to our system and to investigate and contain the incident. We retained a third-party security firm to conduct an independent investigation and to assist in the remediation of our system and implement additional security measures. As such, we have

already strengthened our systems, and will continue to do so. We have removed the unauthorized person from our systems and eliminated the vulnerability that was used to gain access to our systems. We are not aware of any identity fraud or improper use of any personal information directly resulting from this incident, but out of an abundance of caution, we have arranged to have Equifax provide you with two (2) years of complimentary credit monitoring and identity theft protection services.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

- Regularly review and monitor all of your account statements and credit history to guard against any unauthorized transactions or activity.
- Contact your financial institution immediately if you discover any suspicious or unusual activity on your accounts.
- Do not save login/financial credentials in browsers, and keep credentials in a secure location.
- Be careful about what information you post online, and restrict access to your personal details on social media.
- Ensure you have enabled the privacy safeguards on your devices and social media accounts, and keep them enabled.
- Do not access online banking or other sensitive information from public or shared network computers.
- Use only secure networks to conduct work or other important or sensitive transactions.
- When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the website's address starts with "https", instead of just "http", and has a padlock icon in the URL field.
    - This indicates that the website is secure and uses encryption to scramble your data so it cannot be intercepted by others.
    - Also, be on the lookout for websites that have misspellings or bad grammar in their addresses—they could be copycats of legitimate websites.

For More Information:

We deeply regret any inconvenience or concern this incident may cause you. If you have any questions about this notice or the incident, please contact the telephone support center at 888-414-0810 which is available Monday through Friday, 9am – 9pm Eastern time.

Thank you for your understanding.

Sincerely,

Linda Skorb
Vice President, Human Resources

<FIRST NAME> <LAST NAME>
Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

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 information, 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 *<ACTIVATION 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 information 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 information 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.

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.identitytheft.gov

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

Maryland: You may contact the data owner at:

Mativ Holdings, Inc.
ATTN: Legal Department
100 North Point Center East,
Suite 600,
Alpharetta, GA 30022
888-414-0810

You may also 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

Massachusetts: Under Massachusetts 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: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact the data owner at:

Mativ Holdings, Inc.
ATTN: Legal Department
100 North Point Center East,
Suite 600,

Alpharetta, GA 30022
888-414-0810

You may also 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

Washington: The data security incident was discovered on July 9, 2022**.**

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.

Appendix 2
Mativ US (non-Massachusetts – Child Monitoring Credit Watch Gold) Letter Template

<Return Name>
<Return Address>
<City> <State> <Zip>

Parent or Guardian of <FirstName> <LastName>
<Address1>
<Address2>
<Address3>
<City><State><Zip>

<<Date>>

Subject: Notice of Data Incident

Dear Parent or Guardian of <<First Name>>,

We are writing to share with you important information regarding a data incident that potentially involved your child's personal information. We take this incident very seriously and are providing you with information, as well as access to resources, so that you can better protect your child's personal information and diligently monitor your child's accounts.

What Happened:

Through recent investigations, it has become apparent that for a period of time during June and July of this year, an unauthorized person blocked our access to parts of our network and systems and may have gained access to the personal information of the employees and dependents of the legacy Schweitzer-Mauduit International, Inc. ("SWM") and Scapa Group, Ltd. ("Scapa") companies within the Mativ Holdings, Inc. group. As soon as we became aware of the incident, we disconnected the affected IT networks from the internet, and a third-party security firm was engaged to assist with an investigation into the incident.

What Information was Involved:

The investigation was unable to determine what personal information, if any, the unauthorized person actually viewed. In an abundance of caution, we reviewed the information potentially accessed by the unauthorized person and, on August 12, 2022, determined that the unauthorized person may have accessed personal information about the dependents of certain employees, including, potentially, your child. This is because you (or your child's other parent or guardian) as a legacy SWM or Scapa company employee provided us with limited information relating to your dependent(s). The potentially affected information can include the following: date of birth, limited medical information, financial account number, and Social Security number.

What We are Doing:

Immediately upon learning of the incident, we took steps to ensure that the unauthorized person no longer had access to our system and to investigate and contain the incident. We retained a third-party security firm to conduct an independent investigation, and to assist in

the remediation of our system and implement additional security measures. As such, we have already strengthened our system, and will continue to do so. We have removed the unauthorized person from our systems and eliminated the vulnerability that was used to gain access to our systems. While we are not aware of any identity fraud or improper use of any personal information directly resulting from this incident, out of an abundance of caution, we have arranged to have Equifax provide your child, with two (2) years of complimentary credit monitoring and identity theft protection services.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your child's account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your child's accounts, please contact your financial institution. We have provided additional information below, regarding steps you can take to protect your child against fraud and identity theft.

- Regularly review and monitor all of your child's account statements and credit history to guard against any unauthorized transactions or activity.
- Contact your financial institution immediately if you discover any suspicious or unusual activity on your child's accounts.
- Do not save login/financial credentials in browsers, and keep credentials in a secure location.
- Be careful about information you or your child post online, and restrict access to your child's personal details on social media.
- Ensure you have enabled the privacy safeguards on your child's devices and social media accounts, and keep them enabled.
- Do not access online banking or other sensitive information from public or shared network computers.
- Use only secure networks to conduct work or other important or sensitive transactions.
- When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the website's address starts with "https", instead of just "http", and has a padlock icon in the URL field.
    - This indicates that the website is secure and uses encryption to scramble your data so it cannot be intercepted by others.
    - Also, be on the lookout for websites that have misspellings or bad grammar in their addresses—they could be copycats of legitimate websites.

For More Information:

We deeply regret any inconvenience or concern this incident may cause you and your child. If you have any questions about this notice or the incident, please contact the telephone support center at 888-414-0810 which is available Monday through Friday, 9am – 9pm Eastern time.

Thank you for your understanding.

Sincerely,

Linda Skorb
Vice President, Human Resources

Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

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 *<ACTIVATION 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.

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 child's account statements and free credit reports for any unauthorized activity. You may obtain a copy of your child's credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your child's 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 your child is the victim of identity theft or have reason to believe your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your child's 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 child's 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 child's 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.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your child's credit report to put your child's creditors on notice that your child 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 child's 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 child's credit report if your child has already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your child's credit report for seven years.

To place a fraud alert on your child's 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.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your child's credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your child's name. That's because most creditors need to see your child's credit report before they approve a new account. If they can't see your child's report, they may not extend the credit.

How do I place a freeze on my child's 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 child's 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 child's 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 your child is applying for credit or a job, and you can find out which credit bureau the business will contact for your child's 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

Maryland: You may contact the data owner at:

Mativ Holdings, Inc.
ATTN: Legal Department
100 North Point Center East,
Suite 600,
Alpharetta, GA 30022
888-414-0810

You may also 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

Massachusetts: Under Massachusetts 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 child's state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact the data owner at:

Mativ Holdings, Inc.
ATTN: Legal Department
100 North Point Center East,
Suite 600,
Alpharetta, GA 30022
888-414-0810

You may also 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 child's 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

Washington: The data security incident was discovered on July 9, 2022**.**

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