THOMPSON HINE

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

October 27, 2022

VIA OVERNIGHT MAIL

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

Re: Cyber Incident Notification

Dear Attorney General Formella:

This communication serves as notice, on behalf of our client Multi-Color Corporation ("MCC") of a recent cybersecurity incident that affects at least twenty-one (21) New Hampshire residents.

As background, MCC is a manufacturing organization with its headquarters at 4053 Clough Woods Drive, Batavia, OH 45103. On September 29, 2022, MCC 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. MCC immediately deployed security measures to contain and mitigate the threat and retained an external incident response team to accelerate recovery efforts and restore its networks and systems to a normal state of operation. As part of MCC's response efforts, the company engaged leading security experts to further investigate the matter and to help assess the scope of the cyberattack. MCC learned during the investigation that personnel files and other "HR" data were compromised. The information that was involved relates to current and former employees, and potentially their beneficiaries and dependents, and includes sensitive personal information.

On October 26, 2022, MCC began notifying all individuals whose personal data may have been affected by this incident, which included at least twenty-one (21) New Hampshire residents. The aforementioned notifications were in substantially the same form as the attached letter (See Enclosure). MCC's notification to the 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. MCC has offered each impacted individual **complimentary credit monitoring services for two (2) years** through Equifax. MCC has further established a dedicated call support line and website to answer any questions that impacted individuals may have about this incident.

Because MCC had established a comprehensive security program prior to this incident, it has been able to remediate this security incident in a timely manner. With ongoing guidance from independent third-party IT security consultants, MCC continues to analyze the incident and its information security programs. MCC 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)

Multi-Color Corporation
4053 Clough Woods Drive
Batavia, OH 45103

[INSERT DATE]

<<AFFECTED PARTY>>
<<ADDRESS>>
<<CITY, STATE ZIP>>

Re: Notification of Data Breach / Cybersecurity Incident

Dear <<AFFECTED>>,

Multi-Color Corporation ("**MCC**") understands the importance of cybersecurity and protecting your personal data. Unfortunately, the purpose of this letter is to inform you that MCC was the victim of a cyberattack and your personal data within our custody was compromised during the incident. However, 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. Yet, out of an abundance of caution, MCC is providing you complimentary credit monitoring and identity theft protection services and we encourage you to enroll in these services.

What Happened

On September 29, 2022, MCC identified unusual activity occurring within our information networks and systems and discovered that a third party had unauthorized access to our information technology environment. MCC immediately deployed security measures to contain and mitigate the threat and retained an external incident response team to accelerate our recovery efforts. Because of the substantial security controls implemented prior to the cybersecurity incident, we were able to contain the threat within a few hours and become fully operational again within days. However, as part of our investigation, we discovered that the perpetrator of the attack accessed MCC files and records, including proprietary information and personal data related to our employees.

What Information Was Involved

The MCC files and records that were compromised as part of this cybersecurity incident included personnel files and other HR-related data on our employees. Accordingly, the types of personal data on our employees that were compromised in this cybersecurity incident included the following: employee names, dates of birth, email addresses, mailing addresses, telephone numbers, social security numbers, driver's license numbers, and similar government-provided identifiers, healthcare and health insurance-related data, and certain tax withholding and similar financial data.

In some, limited circumstances, employees retained "personal" files on MCC computers and shared-folders that were unrelated to MCC business activities (e.g., personal pictures, applications, records), and this data may also have been compromised.

However, based on the measures that we have implemented and the actions we have taken, there is no indication that personal data subject to this cybersecurity incident has been misused or will be misused in the future.

What We Are Doing

MCC has taken action to remediate this cybersecurity incident and help prevent future occurrences. Given the comprehensive information security program that MCC had established prior to this incident, we were able to

return to a normal state of operations in a timely manner. We have retained independent third-party IT security consultants to analyze the incident, including our information security programs and tools and the status of our data security hygiene. In addition, we proactively notified the Federal Bureau of Investigation, and filed incident reports with certain state regulatory authorities, regarding the nature and scope of this cybersecurity incident. For our employees located outside the United States, we have notified applicable foreign data protection regulators, such as the applicable supervisory authorities in the European Union, the United Kingdom, and in Australia.

Credit Monitoring Services

To help address any concerns you may have, MCC will provide you with complimentary credit monitoring and identity theft protection services for **24 months** offered through Equifax. The enclosed sheet provides instructions for enrollment in these **Equifax Credit Watch™ Gold** services.

What You Can Do

Although there is no indication that personal data subject to this cybersecurity incident has been misused or will be misused in the future, there are several steps that you can take to better protect yourself and your personal data more generally. We recommend you remain vigilant and regularly review your credit card bills, bank statements, and credit reports for any unauthorized activity. Promptly report incidents of suspected identity theft or fraud to your local law enforcement agency, the Federal Trade Commission, your state Attorney General, your financial institution, and to one of the three nationwide consumer reporting agencies to have such incidents removed from your credit file. You should change your passwords regularly, and refrain from using easily guessed passwords and re-using the same passwords for multiple accounts. Be vigilant against third parties attempting to gather information by deception, and exercise extreme caution when clicking on unknown or suspicious website links. See the attachment for additional information with respect to certain security services that may be available to you.

Point of Contact

We have established a dedicated call center to answer questions you may have about this incident, which you can reach at 888-291-2363, from Monday – Friday, 9:00 am to 9:00 pm (Eastern Standard Time). We have also established a dedicated website about this incident that includes a Frequently Asked Question (FAQ) section, and it is available at https://www.mcclabel.com/en/data-security-notice.

****

MCC recognizes the importance of data privacy and information security, and we deeply regret that this cybersecurity incident occurred. From the start, we moved quickly to contain the incident and conducted a thorough investigation with the assistance of leading security experts. We are working hard to ensure that individuals impacted by this incident have answers to questions about their personal data.

Sincerely,

Kevin Kwilinski
President & Chief Executive Officer

mcc

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 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.

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, New York, 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.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.
  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.
- 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.

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:

- 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.

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®

<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.*