NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

December 21, 2020

Via FedEx Overnight

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Chris Cwalina
Partner
Direct line 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

Pursuant to N.H. RSA § 359-C:20(I)(b), I am writing on behalf of my client, ColorTech, Inc. ("ColorTech"), to inform you that ColorTech was the target of a ransomware attack that exposed the personal information of approximately one (1) New Hampshire resident. By providing this notice, ColorTech does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

On October 18, 2020, ColorTech was alerted that portions of its environment had been infected with ransomware. ColorTech immediately contained the incident and launched an investigation. ColorTech also engaged a leading cybersecurity and forensic firm and notified the Federal Bureau of Investigation.

The investigation determined that the unauthorized actor gained access to certain ColorTech systems and exfiltrated data via MEGAsync from ColorTech's file servers prior to execution of the ransomware. ColorTech conducted a thorough review of the evidence related to the data exfiltration and notified affected individuals on November 25, 2020. No New Hampshire residents were affected. Two days before the initial notification to affected individuals was sent, ColorTech obtained new evidence suggesting additional data had been exfiltrated. ColorTech proceeded with notification to known affected individuals to ensure they could take steps to protect themselves. ColorTech has now completed its investigation and on December 16, 2020, ColorTech completed its review of the additional evidence and determined that additional individuals had been affected by the incident. The type of data stolen by the ransomware group included the following types of personal information: name, address, date of birth, and Social Security number.

We are not aware of any fraud or misuse of any personal information as a result of this incident. We do not believe personal information was targeted by the threat actor for the purpose of identity theft, but rather, such information happened to be included in the documents taken by the threat actor as part of the ransomware attack to extort the company. It is important to note that ColorTech did not need the decryptor tool as ColorTech's business continuity and disaster

recovery plans enabled the company to recover from backup processes without the need for the decryptor tool.

To help prevent a similar incident from occurring in the future, ColorTech implemented additional security measures designed to enhance the security of its network, systems and data, including deploying end point detection and response tools to monitor and quickly mitigate threats to ColorTech's network, a forced password reset and strengthening security awareness training. In addition, ColorTech continues to review its security measures, internal controls, and safeguards and to make changes to help prevent a similar incident from occurring in the future.

ColorTech will notify the impacted New Hampshire resident on December 22, 2020 and will be offering the individual 24 months of complimentary credit monitoring and fraud protection services. Enclosed is a sample copy of the letter.

If you have any questions or need further information regarding this incident, please contact me at (202) 662 4691 or chris.cwalina@nortonrosefulbright.com.

Very truly yours,

Chris Cwalina

CGC/

Enclosure

December 22, 2020

[Name]
[Address]
[City, State, Zip]

RE: Notice of Data Security Incident

Dear [Name]:

We are writing in follow up to our December 1, 2020, email regarding the criminal ransomware attack perpetrated against Colortech, Inc. ("Colortech") in October 2020. Our investigation recently determined that the incident may have affected your personal information. This notice describes what we know, steps we have taken in response to the incident, and additional actions you may take to protect yourself.

What Happened

In October 2020, cyber criminals gained access to Colortech's network and stole certain files from Colortech's environment before deploying ransomware across the Colortech network. Upon discovering the attack, we promptly took steps to restore and secure our systems, began an investigation into the nature and scope of the incident, and engaged a leading cybersecurity forensics firm. We also notified federal law enforcement.

In November 2020, we notified the individuals our investigation had determined may have been affected by the incident. However, our investigation recently determined additional information had been stolen from our systems during the attack. Our analysis of the additional information revealed that some of your personal information was contained in the stolen files.

We are not aware of any fraud or misuse of any personal information as a result of this incident. We do not believe personal information was targeted by the threat actor for identity theft purposes, but rather, such information may have been included in documents taken by the threat actor as part of the ransomware attack in an attempt to extort Colortech.

What Information Was Involved

The personal information contained in the potentially stolen files may include your name and one or more of the following: Social Security number, address, and date of birth.

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. We take the protection of your information very seriously. We have also implemented additional security protocols designed to protect our network and systems to prevent a similar type of incident from occurring in the future.

As an added precaution we are offering a complimentary two-year membership of Experian's® IdentityWorks℠ Credit 3B. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: March 31, 2020
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks Credit 3B online, please contact Experian's customer care

team at 877.890.9332 by March 31, 2020. Be prepared to provide the engagement number B007789 as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 24-Month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks, and the 24-month service is offered at no cost to you.

You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit-related fraud.
- **Experian IdentityWorks ExtendCARETM**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic funds transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do

We also recommend that you remain vigilant with respect to reviewing your account statements and credit reports and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the U.S. Federal Trade Commission ("FTC"). Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the FTC regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information.

The security of your personal information is important to us, and we sincerely regret that this incident occurred. For more information, please contact Rhonda Bailey by email at rbailey@colortech.com or by telephone at 423-839-2701.

Sincerely,

Jason Spoone
Director of Finance
Colortech, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information About Identity Theft Protection Guide

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

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain further information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. 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. You may obtain further information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, ncdoj.gov, 877-566-7226.

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.