MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

3 Allied Drive, Suite 303
Dedham, MA 02026

October 25, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Full Color, Inc. ("Full Color") located at 7950 Carr St., Dallas, TX 75227 and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately thirteen (13) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Full Color 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.

Nature of the Data Event

On or about April 13, 2023, Full Color learned of suspicious activity relating to its e-commerce website at www.fullcolor.com. Upon learning of the activity and with the assistance of external cybersecurity specialists, Full Color quicky began investigating the full scope, nature, and impact of the event and confirming the integrity of Full Color's website. The investigation determined that unauthorized actors injected malicious codes into Full Color's website that could have allowed the actors to acquire payment card information used or stored on Full Color's website between December 9, 2022, and May 25, 2023. Full Color since has worked with specialists to remediate this malicious activity fully. Although the investigation could not determine if the unauthorized actors obtained any payment card information, in an abundance of caution, Full Color conducted a thorough and comprehensive review to determine which customers could have been affected. This review was recently completed, and Full Color worked to notify promptly any potentially affected individuals.

The information potentially accessible during the event includes
.

Notice to New Hampshire Residents

On or about October 25, 2023, Full Color provided written notice of this event to approximately thirteen (13) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Full Color moved quickly to investigate and respond to the event, assess the security of Full Color systems, and identify potentially affected individuals. Full Color is also working with subject matter specialists to implement additional enhanced technical safeguards. Additionally, Full Color is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Full Color is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Full Color is providing written notice of this event to relevant state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/dle
Enclosure

EXHIBIT A

FULL COLOR

Return Mail Processing
PO Box 999
Suwanee, GA 30024

10 1 2776 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

October 25, 2023

Notice of [Extra1]

Dear Sample A. Sample:

Full Color, Inc. ("Full Color") is writing to inform you about an incident that may affect the security of your payment card information. This letter provides information about the incident, Full Color's response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened. On or about April 13, 2023, Full Color learned of suspicious activity relating to its e-commerce website (www.fullcolor.com). Upon learning of the activity and with the assistance of external cybersecurity specialists, Full Color quickly began investigating the full scope, nature, and impact of the activity and confirming the integrity of Full Color's website. The investigation determined that unauthorized actors injected malicious codes into Full Color's website that could have allowed the actors to acquire certain payment card information used on Full Color's website between December 9, 2022, and May 25, 2023. Full Color worked with specialists to remediate the malicious activity. Although the investigation could not determine if the unauthorized actors obtained any payment card information, in an abundance of caution, Full Color conducted a thorough and comprehensive review to determine which payment cards could have been affected. This review recently concluded, and you are receiving this letter because the investigation determined that your payment card information may have been affected as a result of this incident.

What Information Was Involved. Full Color's investigation determined that the malicious codes introduced into its website could have been used to capture certain payment card information used on its website during the potential exposure window, including .

What We Are Doing. Full Color treats its responsibility to safeguard customer information as an utmost priority. Full Color has implemented additional enhanced security measures to protect customers' and users' information. Full Color is also working with external subject matter specialists to secure its website further moving forward to reduce the likelihood of similar future incidents. Full Color continues to review its security policies and procedures as part of its ongoing commitment to information privacy and security on an ongoing basis. Full Color is providing notice of this incident to potentially impacted individuals and to state regulators, where required.

What You Can Do. Full Color encourages you to remain vigilant against incidents of identity theft and fraud, review your account statements, monitor your credit reports for suspicious activity, and report any suspicious activity promptly and without delay to your bank or financial institution. Additional information and resources are included in the enclosed "*Steps You Can Take To Protect Personal Information*."

For More Information. Full Color regrets any concern or inconvenience this situation has caused you and understands that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays) by . Please be prepared to provide your engagement number . You may also write to us at: 7950 Carr St., Dallas, TX 75227.

Sincerely,

Full Color, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been

a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this incident. There are approximately four (4) Rhode Island residents that may be impacted by this incident.