McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

April 1, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: American Society for Clinical Pathology – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents American Society for Clinical Pathology ("ASCP"). I am writing to provide notification of an incident at ASCP that may affect the security of personal information of approximately 138 New Hampshire residents. ASCP's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, ASCP does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

ASCP was recently informed that its e-commerce website was the target of a cybersecurity attack that, for a limited time period, potentially exposed payment card data as it was entered on the website. ASCP engaged external forensic investigators and data privacy professionals and conducted a thorough investigation into the incident. As a result of its investigation, on March 11, 2021, ASCP determined that a limited number of residents used a payment card on the website between March 30, 2020, and November 6, 2020. As a result, payment card information may have potentially been exposed, including some or all of the following: the affected residents' names, credit or debit card numbers, card expiration dates, and CVVs.

To date, ASCP has no evidence that any payment card information has in fact been misused. Nevertheless, out of an abundance of caution, ASCP wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. ASCP is providing the affected residents with written notification of this incident commencing on or about April 1, 2021, in substantially the same form as the letter attached hereto. ASCP is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to review their financial account statements for fraudulent or irregular activity on a regular basis and to contact their banks or card issuers as

soon as they see any suspicious transactions. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At ASCP, protecting the privacy of personal information is a top priority. ASCP resolved the issue that led to the potential exposure on the website. ASCP implemented additional security safeguards to protect against future intrusions. ASCP continues ongoing intensive monitoring of its website, to ensure that it exceeds industry standards to be secure of any malicious activity. In addition, ASCP does not store usable payment card data on its website, which greatly limits the potential risk of exposure.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

ASCP **STRONGER**TOGETHER

[redacted]

[redacted]

[redacted]

Dear [redacted],

American Society for Clinical Pathology (ASCP) is writing to inform you of a recent incident that may have affected a limited number of our customers' payment card data used at www.ascp.org.

What Happened?

We have recently been informed that our e-commerce website was the target of a cybersecurity attack that, **for a limited time period, potentially** exposed payment card data as it was entered on our website. We engaged external forensic investigators and data privacy professionals and conducted a thorough investigation into the incident.

What Information Was Involved?

As a result of our investigation, on March 11, 2021, we determined that you used a payment card on the website between the following date(s): [redacted]. As a result, some of your payment card information **may have potentially** been exposed, including some or all of the following: name, credit or debit card number, card expiration date and CVV (3 or 4 digit code on front or back of card) for your payment card(s) ending in [redacted].

Please note, **we have no evidence that your payment card information has in fact been misused,** but we wanted to alert you of this incident so that you can take certain measures if you feel it's necessary to protect your information.

What We Are Doing?

We greatly value our relationship with you, and want to let you know what we are doing to further secure your information. We resolved the issue that led to the potential exposure on the website. We implemented additional security safeguards to protect against future intrusions. We continue ongoing intensive monitoring of our website, to ensure that it exceeds industry standards to be secure of any malicious activity. In addition, **we do not store usable payment card data on the website,** which greatly limits the potential risk of exposure.

What Are Your Options?

Below you will find precautionary measures you can always take to protect your personal information. Additionally, best practices include being vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis and contacting your bank or card issuer as soon as you see any suspicious transactions.

The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You may also ask your bank or card issuer whether a new card should be issued to you.

For More Information

If you have any further questions regarding your potential exposure during this incident, please feel free to call our dedicated and confidential toll-free response line to respond to questions at [redacted]. This response line is staffed with professionals knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

Your trust is a top priority for ASCP and we apologize if this caused you any inconvenience. Especially during these unprecedented times, **we remain committed to the protection of your information.**

Thank you,

ASCP Customer Service

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/
1-800-349-9960	1-888-397-3742	securityfreeze
		1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.