LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
429 Fourth Avenue, Suite 805
Pittsburgh, Pennsylvania 15219
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

April 27, 2021 File No. 44629.68

VIA ELECTRONIC MAIL

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
SecurityBreach@atg.wa.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Ferguson:

Lewis Brisbois Bisgaard & Smith LLP represents the Nexelis Group ("Nexelis") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to serve as a supplemental notice to the Office of the Attorney General Consumer Protection Division of the incident in accordance with Wash. Rev. Code §§ 19.255.005–.040.

I. Nature of the Incident

On November 8, 2020, Nexelis discovered that it had experienced a data security incident disrupting access to certain of its systems. In response, Nexelis took immediate steps to secure its systems and launched an internal investigation which revealed that the disruption was due to a ransomware event. Accordingly, Nexelis retained Lewis Brisbois Bisgaard & Smith LLP to provide legal counsel and, through counsel, engaged an independent digital forensics firm to conduct an investigation to determine what happened and to identify any personal information that may have been accessed or acquired without authorization as a result. Nexelis retained a third-party vendor to complete a thorough review of the impacted information which was completed on March 8, 2021. Nexelis' investigation into the impacted information determined that files containing certain residents' personal information may have been acquired by an unauthorized third-party in connection with this data security incident.

We then worked to determine addresses and mailed letters to affected individuals on April 8, 2021. Thereafter, additional addresses for affected individuals were located and, as a result, a second mailing was sent on April 27, 2021. Although Nexelis is not aware of any misuse of personal

information as a result of this incident, Nexelis decided to provide notification of this incident to individuals whose information may have been impacted.

II. Type of Information and Additional Number of Washington Residents Involved

As previously reported, Nexelis notified 929 residents of this incident on April 8, 2021. Subsequently, on April 27, 2021, Nexelis notified another 28 residents via the enclosed sample letter. The letter provided notified individuals with information pertaining to steps to be taken to help protect personal information and instructions on how to enroll in complimentary identity theft protection services. The services offered varied depending on the information that may have been involved for each individual.

The information involved in the incident differed depending on the individual but for the notified Washington residents, it may have included: Social Security numbers, date of birth, driver's license, health insurance and medical information, digital signature, payment card information, passport number and email address and password for non-financial electronic accounts.

III. Steps Taken Relating to the Incident

As soon as Nexelis learned of the incident, it took immediate steps to secure its systems and launched an investigation. In addition, it implemented measures to enhance the security of its environment in an effort to minimize the likelihood of a similar event from occurring in the future. Nexelis also reported the incident to the FBI and the Royal Canadian Mounted Police and will assist their investigation into the matter.

As discussed above, Nexelis also notified a total of 957 Washington residents of the incident and has provided them with information pertaining to steps they can take to protect their personal information and instructions on how to enroll in complimentary identity theft protection services.

IV. Contact Information

Nexelis is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Lauren.Godfrey@lewisbrisbois.com or 412.567.5113

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

CC: Julie Hess (Julie.Hess@lewisbrisbois.com)

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Nexelis is writing to inform you of an incident that may have involved your personal information. At Nexelis, we take the privacy and security of the information in our possession very seriously. That is why we are contacting you and informing you about this incident and steps you can take to help protect your information.

What Happened? On November 8, 2020, we discovered that some of our systems had been encrypted by malware. We immediately initiated an investigation and engaged cybersecurity experts to assist with the process. On March 8, 2021, after a thorough review of the impacted information, we determined that your personal information was involved in the incident. The information was contained on the server of a company that Nexelis recently acquired, Pacific Biomarkers, that was accessed without authorization from September 26, 2020 to November 9, 2020. Prior to Nexelis' acquisition, Pacific Biomarkers was a laboratory services provider supporting clinical studies in the pharmaceutical industry. The information involved appears to have been related to clinical studies in which you participated in approximately the mid-1990s.

Nexelis has no information to suggest that your personal information has been misused. Nonetheless, out of an abundance of caution, Nexelis has made arrangements to offer you complimentary identity monitoring services for a period of twelve (12) months at no cost to you.

What Information Was Involved? The information may have involved your <<b2b_text_1 (Impacted Data)>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation as well as the Royal Canadian Mounted Police, and will provide whatever cooperation is necessary to help prevent fraudulent activity and facilitate prosecution of the perpetrators. We are also offering you a 12-month identity monitoring service and providing you guidance on steps you can take to help protect your personal information.

What You Can Do. You can enroll in the complimentary 12 months of identity monitoring services being offered by Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
You have until **July 14, 2021** to activate your identity monitoring services.
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter. Please also review the guidance included with this letter about how to further protect your information.

For More Information. If you have questions or need assistance, please call 1-855-723-1663 from 8:00 a.m. to 5:00 p.m. Pacific, Monday through Friday. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Raymond E. Kaiser PhD
Chief Operating Officer

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission,** 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General **Bureau of Internet and** **Technology Resources**	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
28 Liberty Street	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
New York, NY 10005	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
ifraud@ag.ny.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
1-212-416-8433	1-888-743-0023	1-877-566-7226	401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.