16239

SUMMIT BIOSCIENCES INC.
Quality, Integrity and Passion

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 13, 2019

NOTICE OF DATA BREACH AND WHAT'S BEING DONE TO PROTECT YOUR INFORMATION

Dear <<First Name>> <<Last Name>>,

Summit Biosciences Inc. ("Summit") takes the protection and proper use of your information very seriously, which is why we are writing to tell you about a data security incident that may have exposed some of your personal information.

What happened?

On November 7, 2019, Summit became aware that an employee's email was accessed by an unauthorized party. Summit IT immediately took measures to force password changes for all employees' accounts, verify that all email accounts were secure and began investigating the details of the incident. After further examination of the compromised email account, on November 18, 2019, Summit discovered that some personal information may have been available to the unauthorized party.

What information was involved?

Although we do not have evidence that the information was viewed, downloaded, or transferred, we are assuming that any information contained in the employee's email inbox was compromised. Such information may have included first and last name, social security number, date of birth, driver's license number, passport number, and US permanent residence number. It did not include your password or credit card information (which we do not collect). At this time, there is no evidence that your information has been misused.

What we are doing?

Summit values your privacy and deeply regrets that this incident occurred. Our information technology team is conducting a thorough review of the scope of records affected, has required a reset of passwords, installed Multi-Factor Authentication for additional security on critical email accounts, has added alerting reports for any successful logins from unknown locations, and has implemented additional Cybersecurity training for all Summit personnel.

To further assure the protection of your information, Summit is notifying the Attorney Generals offices and/or law enforcement agencies of states where affected individuals reside in accordance with state notification laws.

To help relieve concerns, we have also secured the services of ID Experts® to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Please note that the services of ID Experts are intended to protect your personal information and monitor your personal credit.

What can you do?

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling **1-800-939-4170** or going to https://app.myidcare.com/account-creation/protect and using the personalized Enrollment Code provided at the top of this letter. MyIDCare experts are available Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Standard Time (excluding holidays). **Please note the deadline to enroll is March 13, 2020.**

We encourage you to take full advantage of this service offering even if there is no indication that the information has been illegally used. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Summit did not file a police report in this case. However, had we filed one, we are required to let you know that you would be entitled to request a copy of such report.

Please also review the enclosed "*Additional Resources*" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

You will find detailed instructions for enrollment on the enclosed *Additional Resources* document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so **please do not discard this letter**.

Protecting your information is important to us. We appreciate the trust you place in us and apologize for the inconvenience and understandable concern this incident may cause. We hope that the services we are offering to you demonstrate our continued commitment to your security. Based on what we have learned from this incident we are making additional significant investments in our website and its security to further strengthen its defenses and protect your information.

Sincerely,

Summit Biosciences Inc.

ADDITIONAL RESOURCES
STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

Telephone. Contact MyIDCare at **1-800-939-4170** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Review Your Account Statements and Notify Your Financial Institution and Law Enforcement (if necessary) 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Obtain and Monitor Your Credit Report. We recommend that you 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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	*Experian*	*TransUnion*
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report. We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. A comprehensive guide from the FTC to help you guard against and deal with identity theft can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: (502) 696-5300.

Maryland residents: You can contact the Maryland Attorney General at 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; or by sending an email to idtheft@oag.state.md.us; or calling (410) 576-6491. You may also wish to review information on how to avoid identity theft at: http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx,

New York residents may wish to review information provided by the New York Attorney General's Bureau of Internet and Technology (BIT) at https://ag.ny.gov/internet/data-breach or by calling (212) 416-8433.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling (877) 566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

Ohio residents may wish to review information provided by the Ohio Attorney General at http://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Identity-Theft/Security-Breaches-and-Compromise-of-Personal-Infor or by calling (800) 282-0515.

OTHER IMPORTANT INFORMATION

Security Freeze. In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, cell phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. 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.