Davis Wright Tremaine LLP

Suite 800
1919 Pennsylvania Avenue N.W.
Washington, D.C. 20006-3401

Christin McMeley
202-973-4264 tel
christinmcmeley@dwt.com

February 22, 2018

New Hampshire Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Report of Data Security Incident

To the New Hampshire Office of the Attorney General, Consumer Protection and Antitrust Bureau:

I represent Santa Cruz Biotechnology, Inc. (Santa Cruz), located at 10410 Finnell St., Dallas TX 75220. Pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), I am writing to notify you of an incident that may have resulted in the unauthorized acquisition of personal information of two residents of New Hampshire. Notice of this incident was mailed to these individuals on February 22, 2018.

On Monday, December 18, 2017, Santa Cruz discovered that a burglary of two computers used for HR functions had occurred in their Santa Cruz office on or around December 17, 2017. Santa Cruz immediately contacted law enforcement and began an investigation into the data stored on the laptop. On January 31, 2018, Santa Cruz discovered that personal information associated with two New Hampshire residents may have been stored on these computers, although that has not been confirmed. Prior to this date, Santa Cruz had no reason to believe residents of New Hampshire would be affected because the company has no employees in the state.

While Santa Cruz cannot confirm that the information of these two New Hampshire residents was contained on the stolen computers and has no evidence to suggest that the information on the computers has actually been or will be accessed as a result of this theft, Santa Cruz has decided to notify potentially affected individuals out of an abundance of caution. It is possible that the following personal information may have been included on the stolen computers: full name, postal address, date of birth, Social Security number, medical and health insurance information, and work-related evaluations.

Santa Cruz has implemented, and continues to implement, additional security controls designed to further safeguard their systems, devices, and the information they contain. These new protections include encrypting laptop and desktop computers that contain sensitive information and enabling software capable of locating, disabling, and remotely destroying data on Santa Cruz computers. Santa Cruz has also notified, and is working with, local law enforcement and the FBI in an attempt to identify the perpetrator(s) and will provide whatever cooperation necessary to do so. As an added precaution, Santa Cruz has arranged to have ID Experts provide credit monitoring and identity repair services for one year at no cost to the affected individuals.

Please contact me should you have any questions.

Sincerely

Davis Wright Tremaine LLP

Christin McMeley

Enclosure: Representative sample notification letter to the New Hampshire residents.

SANTA CRUZ

The Power to Question

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017

To Enroll, Please Call:
800-382-2630
Or Visit:
www.IDExpertscorp.com/protect
Enrollment Code: [XXXXXXXX]

[FIRST NAME, LAST NAME]
[ADDRESS]
[CITY. STATE ZIP CODE]

February 22, 2018

Notice of Data Security Incident

Dear [FIRST NAME, LAST NAME]:

We are writing to inform you of an incident that may have resulted in unauthorized access to and acquisition of your personal information. This letter supplements information you may have previously received and more fully describes what happened and what you should do now. We take the protection and proper use of your information very seriously which is why we are offering you one year of identity protection services, informing you of the actions we have taken in response to the incident, and suggesting steps you may wish to take to further protect your information.

What Happened?

On Monday, December 18, 2017, we discovered that a burglary had occurred in our Santa Cruz office on or around December 17, 2017. We immediately contacted law enforcement and began an investigation in order to determine what happened and what may have been affected as a result. As a result of our investigation, we have determined that two computers were stolen, both of which were used for HR functions, but neither of which are capable of remotely accessing our systems. While it was our general practice to store documents with sensitive personal information about employees and potential employees on our servers and not on the local computers, our investigation has revealed that records containing some personal information was stored on at least one of the computers. While we have no evidence to suggest that your personal information was either accessed or acquired by an unauthorized third party, we recommend that you take advantage of the identity theft protection services we are offering below.

What Information Was Involved?

It is possible that the following personal information may have been accessed and acquired as a result of this incident: full name, postal address, date of birth, Social Security number, medical and health insurance information, and work-related evaluations.

What Are We Doing?

We have implemented, and continue to implement, additional security controls designed to further safeguard our systems, devices, and the information contained within them. These new protections include encrypting laptop and desktop computers that contain sensitive personal information and enabling software capable of locating, disabling, and remotely destroying data on SCBT computers. We have also notified, and are working with, local law enforcement and the FBI in an attempt to identify the perpetrator(s) and will provide whatever cooperation necessary to do so.

As an added precaution, we are offering you the MyIDCare identity theft protection services through ID Experts®, at no cost to you. ID Experts' fully managed recovery services will include: 12 months of Single Bureau Credit Monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will work on your behalf to resolve issues, in the event your identity is compromised.

What You Can Do:

We encourage you to enroll in the ID Experts® service at www.idexpertscorp.com/protect and use the Enrollment Code at the top of this letter. You may enroll by phone if you prefer by calling **800-382-2630**, Monday through Friday from 8 am - 8 pm Eastern Time.

You will find detailed instructions for enrollment on the enclosed "Steps You Can Take To Further Protect Your Information" document. Also, you will need to reference your Enrollment Code when calling or enrolling on the website, so please do not discard this letter.

For More Information:

Further information about how to guard against identity theft appears on the next page. Should you have any questions, please contact us by calling **800-382-2630**.

We deeply regret any inconvenience this may cause you.

Sincerely,

John R. Stephenson
CEO

Steps You Can Take To Further Protect Your Information

Website and Enrollment. Go to www.idexpertscorp.com/protect and follow the instructions for enrollment using your Enrollment Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

Activate the credit monitoring provided as part of your membership with ID Experts, paid for by Santa Cruz Biotechnology. Credit monitoring is included in the membership, but you must personally activate it for it 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, ID Experts will be able to assist you.

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).

File Your Tax Return Early. Consider filing your tax returns as early as possible to minimize the chances of tax-related identity theft. If you believe you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify any questionable activity, please complete *Form 14039, Identify Theft Affidavit*, available at https://www.irs.gov/pub/irs-pdf/f14039.pdf, and submit it to the appropriate address per the form instructions. Additional information on ways you can reduce your risk and steps you can take if you believe you have become a victim of tax-related identity theft can be found in the IRS's *Taxpayer Guide to Identity Theft*, available at https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.

Obtain a Copy of Your 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, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Place a Fraud Alert on Your Credit Report. 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 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.

Place a Security Freeze on Your Credit File. In some US states, you have the right to put a security freeze on your credit file. 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 consumer reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. 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 on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Penn. Ave, NW	200 St. Paul Place	9001 Mail Service Ctr	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

We will NOT send you any electronic communications regarding this incident and ask you to disclose any personal information.