

# REVANCE®

July 10, 2023

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

*Via Email - DOJ-CPB@doj.nh.gov*

To Whom It May Concern:

On behalf of Revance Therapeutics, Inc. ("Revance"), a biotechnology and pharmaceutical company, I am writing to inform you about a recent incident in which personal information relating to New Hampshire residents was accessed by an unauthorized third party. Revance's corporate headquarters is located at 1222 Demonbreun St, Suite 2000. Nashville, TN 37203.

On April 9, 2023, we discovered that an unauthorized third party had accessed certain of our company's systems and exfiltrated certain information. As soon as we became aware of the incident, we terminated the third party's access to the affected systems and immediately began an investigation to determine the scope of the incident and identify the impacted information. We engaged a third-party cybersecurity firm that specializes in incident response to assist with our investigation and ensure that the incident was contained. After additional analysis, on April 27, 2023, we confirmed that the third party accessed and exfiltrated certain personal information from Revance's systems.

We also engaged third-party data review specialists to conduct a detailed review of the exfiltrated data and identify the individuals whose personal information may have been impacted. This review was completed on June 15, 2023.

Through our investigation, we determined that the incident occurred between March 15, 2023, and April 10, 2023, and was caused by the compromise of an employee's credentials. We also determined that the unauthorized third party may have accessed the

relating to current and former company employees and their dependents and certain company vendors or contractors.

In response to this incident, we have enhanced our identity access management controls and authentication controls. We also notified federal law enforcement and cooperated with them throughout the incident response process.

We will notify 2 New Hampshire residents of this incident.

We are not aware of any misuse of information. As a precaution, we have engaged Kroll, Inc. to provide these individuals with an offer for complementary access to of its identity monitoring, which provides a number of services, including Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick

1222 Demonbreun St, 20<sup>th</sup> Floor, Nashville, TN 37203

# REVANCE®

Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. An individual can enroll in the identity monitoring by visiting the website or calling the telephone number provided in their individual notice letter.

Attached is a sample of the letter that we are providing to New Hampshire residents.

Please do not hesitate to contact me at \_\_\_\_\_ if you have any questions. I can also be reached at [gabrielle.white@revance.com](mailto:gabrielle.white@revance.com).

Sincerely,

**Gabrielle Sims White**  
VP, Legal – Lead Corporate Counsel

*Enclosed: Sample Individual Notice Letter*



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

### Notice of Data Breach

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

On behalf of Revance Therapeutics, Inc. (“Revance”), I am writing to inform you about a recent incident that involved personal information about you. Please know that we take the security of your personal information seriously.

**WHAT HAPPENED.** On April 9, 2023, we discovered that an unauthorized third party had accessed and exfiltrated information from certain Revance systems. We immediately began an investigation to determine the scope of and contain the incident. Based on our investigation, the incident occurred between March 15, 2023 and April 10, 2023. After additional analysis, on April 27, 2023, we confirmed that the third party accessed and exfiltrated certain personal information from Revance’s systems.

**WHAT INFORMATION WAS INVOLVED.** We have determined that the personal information involved in this incident included your <<b2b\_text\_1 (name and data elements)>>.

**WHAT WE ARE DOING.** After becoming aware of the incident, we terminated the third party’s access to the affected systems. We began an investigation and engaged third-party cybersecurity specialists to investigate and resolve the incident. We also notified law enforcement. In response to this incident, we have taken steps to enhance the security controls used to help protect your data.

**WHAT YOU CAN DO.** Please note, we are not aware of any misuse of the impacted information. We are providing you with the following information about general steps that you can take to help protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to activate a complimentary two-year identity monitoring service through 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, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

For more information about Kroll and your Identity Monitoring services, you can visit

Additional information describing your services is included with this letter.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s Web site, at [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/), or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit-reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit-reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit-reporting agencies. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
<a href="http://Equifax.com/personal/credit-report-services">Equifax.com/personal/credit-report-services</a>	<a href="http://Experian.com/help">Experian.com/help</a>	<a href="http://Chester, PA 19022">TransUnion.com/credit-help</a>

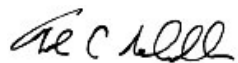
You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: [http://files.consumerfinance.gov/f/201410\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf).

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

**FOR MORE INFORMATION.** Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us if you have any questions or concerns at \_\_\_\_\_, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,



**Tobin Schilke**  
**Chief Financial Officer**

*IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT:* You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

Office of the Attorney General  
441 4th Street, NW  
Suite 1100 South  
Washington, DC 20001  
(202) 727-3400  
<https://oag.dc.gov/>

*IF YOU ARE A MARYLAND RESIDENT:* You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023  
<https://www.marylandattorneygeneral.gov/>

*IF YOU ARE A NEW YORK RESIDENT:* You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

New York Attorney General  
Consumer Frauds &  
Protection Bureau  
120 Broadway, 3rd Floor  
New York, NY 10271  
(800) 771-7755  
[www.ag.ny.gov](http://www.ag.ny.gov)

New York Department of State  
Division of Consumer Protection  
99 Washington Avenue  
Suite 650  
Albany, New York 12231  
(800) 697-1220  
[www.dos.ny.gov](http://www.dos.ny.gov)

*IF YOU ARE A NORTH CAROLINA RESIDENT:* You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

North Carolina Department of Justice  
Attorney General Josh Stein  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
<https://ncdoj.gov/>

*IF YOU ARE A RHODE ISLAND RESIDENT:* We have determined that the incident involved personal information regarding two Rhode Island individuals. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General  
150 South Main Street  
Providence, RI 02903  
(401) 274-4400  
<http://www.riag.ri.gov/>



## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

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

### **TRIPLE BUREAU CREDIT MONITORING AND SINGLE BUREAU CREDIT REPORT**

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

### **WEB WATCHER**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **PUBLIC PERSONA**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

### **QUICK CASH SCAN**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 MILLION IDENTITY FRAUD LOSS REIMBURSEMENT**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **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.