

JONES DAY

51 LOUISIANA AVENUE, N.W. • WASHINGTON, DC 20001.2113

TELEPHONE: +1.202.879.3939 • JONESDAY.COM

DIRECT NUMBER: +1.202.879.5494

JEVERETT@JONESDAY.COM

September 15, 2023

BY E-MAIL

Office of the Attorney General
Attention: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

I am writing on behalf of our client International Business Machines Corporation (“IBM”), a service provider to Johnson & Johnson Health Care Systems, Inc. (“Janssen”), to inform you of a data security incident involving the personal information of residents of Maryland.

This notice concerns an incident involving unauthorized access to personal information contained within a database used on the Janssen CarePath platform, a patient support platform that offers savings options and other patient support resources. IBM manages the application and the third-party database that supports Janssen CarePath.

Janssen recently became aware of a technical method by which unauthorized access to the database could be obtained. Janssen then immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue. IBM also undertook an investigation to assess whether there had been unauthorized access to the database. While IBM’s investigation identified, on August 2, 2023, that there was unauthorized access to personal information in the database, the investigation was unable to determine the scope of that access. As a result, notice is being provided to approximately 66,275 residents of Maryland whose information of the types listed below was contained in the database prior to remediation. IBM also is offering notice recipients the opportunity to enroll in one year of complimentary credit monitoring services.

The personal information in the database may have included individuals’ names and one or more of the following: contact information, health insurance information, and information about medications and/or associated conditions that were provided to the Janssen CarePath application. Social Security numbers and financial account information of users were not involved in this incident.

After being informed of the issue by Janssen, IBM and the database provider promptly identified and implemented steps that disabled the technical method at issue. IBM also worked

Attorney General Brown
September 15, 2023
Page 2

with the database provider to augment security controls to reduce the chance of a similar event occurring in the future.

Attached is a sample of the letter that IBM is providing to Maryland residents. Notice will be provided on a rolling basis by mail, to individuals whose addresses are available. Notice also will be made via substitute notice, consisting of media notice and website posting on the Janssen CarePath website at www.janssencarepath.com.

IBM's corporate headquarters is located at 1 New Orchard Road, Armonk, New York 10504-1722 and Janssen's corporate headquarters is located at 1 Johnson and Johnson Plaza, New Brunswick, New Jersey 08933.

Please do not hesitate to contact me if you have any questions. Johnson & Johnson Health Care Systems, Inc., the owner of Janssen CarePath, is represented by Morrison Foerster and can be reached in care of Miriam Wugmeister at MWugmeister@mofo.com.

Sincerely,

Jennifer C. Everett

Jennifer C. Everett

Encl.

INTERNATIONAL BUSINESS MACHINES CORPORATION

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

This notice concerns an incident involving unauthorized access to personal information contained within a database used on the Janssen CarePath platform, a patient support platform that offers savings options and other patient support resources.

International Business Machines Corporation (“IBM” or “we”) is a service provider to Johnson & Johnson Health Care Systems, Inc. (“Janssen”). IBM manages the application and the third-party database that supports Janssen CarePath. We are writing to inform you of a recent incident that may have involved unauthorized access to your personal information stored in Janssen CarePath. While we have no reason to believe that your information has been misused, we want to let you know what happened and the steps we have taken in response. This letter explains what happened, our response, and steps you can take to protect your information.

What happened: Janssen recently became aware of a technical method by which unauthorized access to the database could be obtained. Janssen then immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue. IBM also undertook an investigation to assess whether there had been unauthorized access to the database. While IBM’s investigation identified, on August 2, 2023, that there was unauthorized access to personal information in the database, the investigation was unable to determine the scope of that access. As a result, we are notifying you out of an abundance of caution.

What information was involved: The personal information involved in this incident may have included your name and one or more of the following: <<Consolidated Breached Elements>>. Your Social Security number and financial account information were not contained in the database or affected.

What we are doing: After being informed of the issue by Janssen, IBM and the third-party database provider promptly identified and implemented steps that disabled the technical method at issue. IBM also worked with the third-party database provider to augment security controls to reduce the chance of a similar event occurring in the future.

What you can do: We encourage you to remain vigilant by regularly reviewing your account statements and explanations of benefits from your health insurer or care providers with respect to any unauthorized activity. If you identify services that you did not receive or other suspicious activity, promptly report that activity to the institution that provided the report. Additional information on steps that you can take to protect against potential misuse of personal information can be found in the enclosed “Additional Resources” document, which we encourage you to review.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary one-year credit monitoring service through **Equifax Complete Premier**. **Equifax Complete Premier** provides services to monitor your personal information online for identity theft. To enroll in **Equifax Complete Premier**, visit www.equifax.com/activate and follow the following steps.

Enter your unique Activation Code of <<**ACTIVATION CODE**>> then click “Submit” and follow these four steps:

1. **Register:** Complete the form with your contact information and click “Continue”. If you already have a myEquifax account, click the “Sign in here” link under the “Let’s get started” header.
Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the Terms of Use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click “Sign Me Up” to finish enrolling.

The confirmation page shows your completed enrollment. Click “View My Product” to access the product features.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Equifax Complete Premier code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Equifax Complete Premier, so please enroll before the deadline.

If you have questions regarding **Equifax Complete Premier**, please call (888) 604-6584.

For more information: We take information security very seriously and 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 (888) 604-6584 Monday through Friday from 9 AM to 9 PM Eastern Time (excluding major U.S. holidays) or visit www.janssencarepath.com to obtain additional information. Please provide the following unique identification number when calling the call center: <<**Unique ID**>>.

Sincerely,

International Business Machines Corporation

ADDITIONAL RESOURCES

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring 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 state 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 website at 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 the nationwide credit reporting agencies. 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 federal law, 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 or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19022-2000
www.TransUnion.com

You also have other rights under the Fair Credit Reporting Act (“FCRA”). For information about your rights under the FCRA, please visit: 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 verify your identity. You may place a fraud alert in your file by calling any of the 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 provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. After receiving your request, the credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze in the future. You should keep the PIN or password in a safe place.

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)
www.ftc.gov/idtheft

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
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)
www.ftc.gov/idtheft

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
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) www.ftc.gov/idtheft	New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3 rd Floor. Suite 650 New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue Albany, New York 12231 (800) 697-1220 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)
www.consumer.gov/idtheft

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

IF YOU ARE A RHODE ISLAND RESIDENT: We are providing notice of this incident to approximately 10,000 Rhode Island residents. 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
www.riag.ri.gov

IF YOU ARE AN IOWA RESIDENT: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

IF YOU ARE A RESIDENT OF OREGON: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: (877) 877-9392.

IF YOU ARE A RESIDENT OF NEW MEXICO: You have rights under the federal FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.