



March 18, 2024

Via E-Mail

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

To Whom It May Concern:

I write on behalf of Johnson Matthey, Inc. (the “Company”) to provide notice of a security incident potentially affecting 10 Maryland residents.

On February 15, 2024, the Company learned that files containing the personal information of members of our U.S.-based workforce had been stored on a third-party storage platform. Upon being made aware of the situation, the Company immediately located the files, removed them from the storage platform and performed an investigation into the incident. Through our investigation, we determined that the files were temporarily placed on the storage platform by a contractor hired to perform work for the Company who inadvertently left the files on the platform following the completion of their work. While our investigation is ongoing, the Company believes the documents may have been stored on the platform since 2020 without access controls. However, the Company has not found any evidence to suggest that the files were accessed or downloaded during this time. Moreover, as part of our investigation into the incident the Company performed searches of the dark web and did not find any of the files—or information contained in the files—stored there.

The Company’s investigation determined that the files stored on the platform included employment-related documents that contained the personal information of Maryland residents, including their name, Social Security number, and date of birth. Please note that we have received no information indicating that the personal information of the Maryland residents has been misused in any way.

Out of an abundance of caution, we have notified all potentially affected Maryland residents and offered them two years identity theft protection services at no cost to them. A template copy of the notification sent to Maryland residents is attached to this letter.

If you have any questions concerning this matter, please do not hesitate to contact our counsel Mr. Kwabena Appenteng at 312-795-3268 or Kappenteng@littler.com.

Very truly yours,

Caroline Burton

Caroline Burton
Global Data Protection Officer
Johnson Matthey, Inc.



Johnson Matthey
Inspiring science, enhancing life

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[NAME]
[STREET ADDRESS]
[CITY], [STATE] [ZIP]

March 18, 2024

Dear [NAME]:

Johnson Matthey, Inc. (the "Company") values its employees and is committed to protecting your personal information. We are writing to inform you of a recent information security incident and to share with you the steps that we are taking to address it.

On February 15, 2024, the Company learned that files containing the personal information of members of our U.S.-based workforce had been stored on a third-party storage platform. Upon being made aware of the situation, the Company immediately located the files, removed them from the storage platform and performed an investigation into the incident. Through our investigation, we determined that the files were temporarily placed on the storage platform by a contractor hired to perform work for the Company who inadvertently left the files on the platform following the completion of their work. While our investigation is ongoing, the Company believes the documents may have been stored on the platform since 2020 without access controls. However, the Company has not found any evidence to suggest that the files were accessed or downloaded during this time. Moreover, as part of our investigation into the incident the Company performed searches of external websites and repositories and did not find any of the files—or information contained in the files—stored there.

We are writing to you because the files stored on the platform included employment-related documents that contained your personal information, including your name, Social Security number and date of birth. We have no information indicating that your personal information has been misused in any way. Also, based on our investigation, we are confident that that the files in question did not contain any of your other sensitive information, such as financial account information.

Nevertheless, out of an abundance of caution, the Company is offering you two years of identity protection services, at no cost to you, through Experian, one of the three nationwide credit bureaus. Your two-year membership in Experian's IdentityWorksSM product provides identity restoration services, fraud detection tools, and other benefits, which include monitoring your credit file at Experian. Enrollment in IdentityWorks will not affect your credit score.

Starting today, you can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until June 30, 2026, by calling Experian at 1-877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate the fraud detection tools available through IdentityWorks. This product provides you with identity detection, credit monitoring, and resolution of identity theft. If you wish to enroll in IdentityWorks, you will need to do the following:

1. **Visit** the IdentityWorks web site: www.experianidworks.com/credit or call 1-877-890-9332 to enroll and provide Engagement Number **[NUMBER]**.
2. **PROVIDE** your Activation Code: **[ACTIVATION CODE]**.

Enrollment Deadline: **June 30, 2024** (your Activation Code will not work after this date).

If you have any questions concerning IdentityWorks, or if you prefer to enroll over the phone for delivery of your membership via U.S. mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number **[NUMBER]** as proof of eligibility for the identity protection product by Experian. Along with the offer of IdentityWorks, we have also included with this letter additional information on steps you can take to protect the security of your personal information. I urge you to review this information carefully.

Please know that the Company takes seriously both the security of your personal information and this incident. In response to our investigation into this incident we have already assessed steps to prevent a recurrence, including a review of our third-party data handling protocols. Law enforcement has not requested that we delay notifying you.

The Company regrets this incident and any inconvenience it may cause you. Should you have any questions or concerns regarding this incident, please do not hesitate to contact our dedicated hotline at **[PHONE NUMBER]** between 8 A.M. and 6 P.M (CST), Monday through Friday.

Sincerely,

Caroline Burton

Caroline Burton
Global Data Protection Officer
Johnson Matthey, Inc.

JOHN-ADT-1

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorks. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks membership. Experian's IdentityWorks product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors your credit files at Experian, Equifax, and Transunion for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorks membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks product to Experian. A credit card is not required for enrollment in IdentityWorks. Enrollment in IdentityWorks will not affect your credit score. The Terms and Conditions for this offer are located at: www.ExperianIDWorks.com/restoration.

2. Review your credit reports. You are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You can also receive free credit reports by placing a fraud alert, described below. Errors in information in your credit report, such as a home address or accounts you do not recognize, may be a sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your credit report, whether or not due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

3. Review your account statements. Although we have no reason to believe that your payment or other financial information was impacted by this incident, you should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorks identity resolution agent toll-free at 1-877-890-9332 or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to the Company, your local police department, your state's attorney general, and the Federal Trade Commission.

5. You have the right to place a "security freeze" on your credit report. A security freeze will restrict access to your credit file, by prohibiting a consumer reporting agency from releasing information in your credit file without your express consent. This will prevent any unauthorized individuals from opening new credit, loans, or other accounts in your name. However, placing a security freeze on your credit file may also delay or make it more difficult for you to request or apply for a new loan, mortgage, or any other account involving the extension of credit.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

A security freeze does not apply to existing accounts you have that request information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

There is no charge to place a security freeze. Don't confuse security freezes with "credit locks" or similar programs—they work in similar ways, but credit locks typically come with monthly fees or other expenses. If you want to freeze your credit for free, as guaranteed by federal law, then opt for a security freeze and not a credit lock.

To place a security freeze on your credit file, contact all three of the nationwide credit bureaus, listed below, either online, by mail, or by phone. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. The contact information for all three credit bureaus is as follows:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-685-1111
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. 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. 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 bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; <http://www.ftc.gov/idtheft/>; (877) IDTHEFT (438-4338).

If you live in Maryland, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

If you live in Massachusetts, please read the additional notice below that applies to you:

Massachusetts law gives you the right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of filing.

If you live in New York, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
www.ag.ny.gov/

If you live in North Carolina, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226 (within North Carolina)
1-919-716-6000 (outside of North Carolina)
www.ncdoj.gov