MORRISON FOERSTER

250 WEST 55TH STREET
NEW YORK
NEW YORK 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

AMSTERDAM, AUSTIN, BERLIN, BOSTON, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, MIAMI, NEW YORK, PALO ALTO, SAN DIEGO, SAN FRANCISCO, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

June 30, 2025

Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504

To Whom It May Concern:

On behalf of our client Johnson Controls, which is engaged in the engineering, manufacturing, and servicing of building products and systems, we are writing to inform you about an incident that involved personal information relating to Washington residents.

As background, on September 24, 2023, Johnson Controls became aware of a cyber incident that involved the disruption of its information technology infrastructure and resulted in an unauthorized actor having access to and taking data stored on Johnson Controls' network. Johnson Controls quickly launched an investigation with the support of leading third-party experts and took steps to prevent further access and remove the actor from the network. In addition, on October 17, 2023, Johnson Controls notified its employees by posting information related to this incident on the company's intranet and offering employees free credit monitoring, including fraud alerting, identity restoration, and identity theft insurance coverage. Johnson Controls also notified law enforcement and publicly disclosed the incident in filings to the U.S. Securities and Exchange Commission on September 27, 2023, November 13, 2023, and December 14, 2023.

Based on the investigation, Johnson Controls determined that an unauthorized actor accessed certain Johnson Controls systems from February 1, 2023 to September 30, 2023 and took personal information, including personal information of Washington residents, from those systems. Johnson Controls believes that this personal information largely related to current and former Johnson Controls employees and contractors. Johnson Controls does not have reason to believe that the impacted information has been used to cause harm to individuals.

Due to the nature and complexity of the data involved, Johnson Controls has been working diligently with a dedicated review team, including internal and external experts, to conduct a detailed and comprehensive analysis of the data that was taken. This process included working to identify the individuals to whom that personal information relates and determining the nature of the personal information.

This review process has recently concluded. Through this review, Johnson Controls determined that the data involved in the incident was primarily information typically held in the context of an employer-employee (or contractor) relationship. In addition, for some individuals, more sensitive personal data was involved.

On June 30, 2025, Johnson Controls began supplementing its initial October 2023 notice by mailing individual notifications to 4,903 Washington residents. As part of this notification, through Equifax, Johnson Controls is offering individuals complimentary two-year credit and identity monitoring services and certain fraud support services. Johnson Controls has also posted updated information related to the incident to its website. Attached is a sample of the letter Johnson Controls is providing to Washington residents.

In response to this incident, Johnson Controls has also taken appropriate steps to enhance its security controls including blocking known indicators of compromise, conducting an enterprise-wide password reset, fortifying its identity and access management protocols, enhancing its security monitoring and logging capabilities, expanding its multi-factor authentication coverage, and reconfiguring security settings across its systems and virtual infrastructure.

If you have any questions, please do not hesitate to contact me at +1 (212) 506-7213. I can also be contacted at 250 West 55th Street, New York, New York 10019 and MWugmeister@mofo.com.

Sincerely,

Miriam Wugmeister
Counsel to Johnson Controls

Johnson Controls

Return Mail Processing Center
102 W Service Rd # 384
Champlain NY 12919

June 30, 2025

ADFFIN T1 B1 P1 AADC c1 00000001

[Name]
[Address]

Notice of Data Breach

On behalf of Johnson Controls, we are writing to provide information related to the cyber incident that Johnson Controls became aware of in September 2023, which involved personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. On September 24, 2023, Johnson Controls became aware of a cyber incident that involved the disruption of its information technology infrastructure and resulted in an unauthorized actor having access to and taking data stored on Johnson Controls' network. We quickly launched an investigation with the support of leading third-party experts and took steps to prevent further access and remove the actor from the network. Based on our investigation, we determined that an unauthorized actor accessed certain Johnson Controls systems from February 1, 2023 to September 30, 2023 and took information from those systems.

WHAT INFORMATION WAS INVOLVED. Given the nature and complexity of the data involved, Johnson Controls has been working diligently with a dedicated review team including internal and external experts to conduct a detailed analysis of the data that was taken from Johnson Controls' network. Based on this data analysis, we believe that the unauthorized actor took information about you including your name and [types of personal information].

WHAT WE ARE DOING. We began investigating the incident as soon as we learned of it. After becoming aware of the incident, we terminated the unauthorized actor's access to the affected systems. In addition, we engaged third-party cybersecurity specialists to further investigate and resolve the incident. We also notified law enforcement and publicly disclosed the incident in filings on September 27, 2023; November 13, 2023; and December 14, 2023. In response to this incident, we have taken appropriate steps to enhance our security controls.

WHAT YOU CAN DO. We do not have reason to believe that the impacted information has been used to cause harm to individuals. Nonetheless, and consistent with certain laws, we are providing you with the following information about steps that you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year credit monitoring service. We have engaged Equifax to provide you with its Equifax Credit Watch™ Gold, which includes credit monitoring, fraud alerts, identity restoration, identity theft insurance coverage and other features, detailed further on the final page of this letter. **You have until October 31, 2025 to activate the free credit monitoring service by using the following activation code: [Activation Code].** This code is unique for your use and should not be shared. To enroll, go to www.equifax.com/activate

00695-ADFFIN-AUTO-00000001- 000001-000-1/2

You should 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 or the relevant entity with which you hold that account. You should also be cautious of any unsolicited communications asking for personal information. In addition, if a username and password are listed among your information above, we recommend that you change your login credentials for online accounts.

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, 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 identify information on your credit report resulting 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	*Experian*	*TransUnion*
(800) 685-1111	(888) 397-3742	(800) 680-7289
P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	P.O. Box 9701 Allen, TX 75013-9701 www.experian.com	Fraud Victim Assistance Department 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: *https://files.consumerfinance.gov/f/201504_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 obtain 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 is required to notify the other two agencies, which then must also place fraud alerts in your file.

You can also 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. The credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift 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. If you have any additional questions or concerns, please go to www.faq.jci.com/english-us or contact us at 1-855-361-0339.

Sincerely,

Johnson Controls

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.consumer.ftc.gov/idtheft

Office of the Attorney General
400 6th Street, NW
Washington, DC 20001
(202) 727-3400
www.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.consumer.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.consumer.ftc.gov/idtheft

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 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.ftc.gov/idtheft

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

IF YOU ARE A RHODE ISLAND RESIDENT: 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

****

EQUIFAX®

[Name]
Activation Code: **[Activation Code]**
Enrollment Deadline: **October 31, 2025**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- *WebScan notifications*[1] *when your personal information, such as Social Security Number, credit/debit card or bank* account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- *Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity* Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **[Activation Code]** then click "Submit" and follow these 4 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.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*