March 27, 2025

[First name], [Last name]
[Street address],
[City], [State], [Postal Code]

Re: Notice of Data Security Incident. Please read this entire letter.

Dear [First name] [Last name],

Smiths Interconnect Americas, Inc ("Smiths") writes to notify you of a recent incident that may have involved personal information about you and your dependents. SIA is in possession of your information because you are, or at one time were, employed by Smiths and may have enrolled in associated benefit plans provided to you. The incident has been contained, and steps have been taken to continue to strengthen our systems and protect your privacy.

There is no evidence that your information has been misused because of this incident. The issue was contained, and we have confidence that the information that was accessed is secure. However, we are providing this notice to you in consideration of certain legal obligations.

What happened
On January 23, 2025, Smiths became aware of a cyber incident and began to investigate promptly.

On February 3, 2025, the investigation determined that the unauthorized third party accessed copies of certain records on Smiths' network containing information related to certain existing and former employees. The issue was contained, and we can say with confidence that the information that was accessed is secure and has not been misused. Accordingly, the risk to you is low.

What information was involved
The following information about you and your dependents may have been impacted: demographic information (such as name and date of birth), contact information, driver's license or other government issued ID, Social Security number or tax ID, financial information, health information, or health insurance information, including information associated with benefits enrollment.

What we are doing
We are conducting dark web monitoring and have implemented additional security measures to reinforce our systems and prevent similar occurrences. In addition, to address our legal obligations, we are offering 2 years of credit monitoring and identity theft protection services through Experian at no cost to you. The enrollment instructions are detailed in Attachment A.

What you can do

In addition to enrolling in the credit monitoring and identity theft protection services, please review Attachment B, “Steps You Can Take to Help Protect Your Information”. Remain vigilant when dealing with any unsolicited or unexpected communications.

For more information

We take the protection of employee information very seriously and regret that this incident occurred. If you have any questions, please contact your local HR representative.

Sincerely,

Smiths Interconnect Americas, Inc

Smiths Interconnect Americas, Inc
2001 NE 46th St, Suite 188, Kansas City,
MO 64116, United States

US: + 1816-801-3100

smithsinterconnect.com
info.us@smithsinterconnect.com

Attachment A – Identity Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll **by** [**date**] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [**Activation Cod**e]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 931-7577** by 30 June 2025. Be prepared to provide engagement number: [number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [24]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files 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 receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

Smiths Interconnect Americas, Inc
2001 NE 46th St, Suite 188, Kansas City,
MO 64116, United States

US: + 1816-801-3100

smithsinterconnect.com
info.us@smithsinterconnect.com

Attachment B – Additional Steps You Can Take to Help Protect Your Information

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of 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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report. You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Under Massachusetts law, you have a right to obtain a police report filed relating to this incident (if any), and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.