Sustainability Business division of Schneider Electric
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<FIRSTNAME> <LASTNAME>
<ADDRESS 1>
<ADDRESS 2>
<City>, <State> <PostalCode+4>

October 31, 2025

Re: Notice of Data Breach

As you may recall, the Schneider Electric Sustainability Business was impacted by a ransomware incident as of January 17, 2024. We are writing to inform you that we have completed our review and determined the incident involved some of your personal information. This letter is to provide you with the details of what happened, the measures we have taken in response, and to recommend additional steps you may consider to help protect your information. As stated in a prior email about this incident, dated March 21, 2024, as a courtesy and out of an abundance of caution, Schneider Electric previously offered you a complementary 24-month membership of monitoring services to help protect your identity.

What Happened?
The Sustainability Business detected a ransomware incident on January 17, 2024, which caused temporary disruptions to some of its systems and operations. Upon detecting the incident, we immediately began an investigation. The investigation determined that certain Sustainability Business division systems were accessed by an unknown, unauthorized actor between December 27, 2023, and January 17, 2024, and during this time unstructured datasets were obtained. We conducted a thorough review of the impacted data to identify what information was involved and identify individuals to whom the data was related.

What did we do?
Promptly after the incident was detected on January 17, the SE Global Incident Response team was mobilized to respond to the attack, contain the incident, and to reinforce existing security measures, with the help of outside expertise. Critical resources were also taken offline as a preventive measure. The incident was contained and affected platforms were brought back online on January 31, 2024.

We worked as quickly as possible to identify and review the affected data and determine which employees and related individuals were affected so we could provide notice. While the dataset that was impacted was a small portion of the Sustainability Business' total data, the data was unstructured which increased the complexity of the review process and necessitated that rigorous analysis to review the documents for any personal information, quality check those materials, and associate that data with the correct individual.

While this type of review took time to carry out, we believe that it was the best way to ensure we have an accurate and comprehensive understanding of the affected data and the impact on employees and related individuals.

What Information Was Involved?
We completed our review and determined that some of your personal information was contained in the files including your name together with the following: <**Exposed Data Elements>**.

What You Can Do
We encourage you to review the additional information on **Transunion Single Bureau Credit Monitoring** including instructions on how to activate your complementary, 24-month membership as follows:

We previously offered you a complementary membership of **Transunion Single Bureau Credit Monitoring**. Although we are not aware of any fraud or misuse of any personal information due to this incident, as a precaution and to address any potential concerns, we are offering you an additional opportunity to sign up for a complementary, 24-month membership of **Transunion Single Bureau Credit Monitoring** if you have not yet exercised that opportunity. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. **Transunion Single Bureau Credit Monitoring** is completely free to you and enrolling in this program will not hurt your credit score.

These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **<UniqueCode>.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age.

Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Please also review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or security freeze on your credit file.

For More Information. The security of your personal information is important to us, and we sincerely regret that this incident occurred. If you have any questions or need additional information about this incident, please email SB.privacy.notification@se.com. <Custom Field 1>

Should you have any questions regarding **Transunion Single Bureau Credit Monitoring**, have difficulty registering, or require additional support in relation to the **Transunion Single Bureau Credit Monitoring**, please contact Cyberscout at 1-833-647-0356.

Sincerely,

<Custom Field 2>
<Custom Field 3>

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 PO Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the
U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies — Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to vvvvw.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports,

contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. 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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-8085318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-7430023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

For Texas Residents: You may contact and obtain information from your state attorney general at:
Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identitytheft
or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Sustainability Business division of Schneider Electric
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<FIRSTNAME> <LASTNAME>
<ADDRESS 1>
<ADDRESS 2>
<City>, <State> <PostalCode+4>

October 31, 2025

Re: Notice of Data Breach

We are writing to inform you of a cybersecurity incident that impacted the Sustainability Business division of Schneider Electric and, based on our thorough review, involved some of your personal information. This letter is to provide you with details of what happened, the measures we have taken in response, and to provide you with details on additional steps you may consider to help protect your information.

What Happened?
The Sustainability Business detected a ransomware incident on January 17, 2024, which caused temporary disruptions to some of its systems and operations. Upon detecting the incident, we immediately began an investigation. The investigation determined that certain Sustainability Business division systems were accessed by an unknown, unauthorized actor between December 27, 2023, and January 17, 2024, and during this time unstructured datasets were obtained. We conducted a thorough review of the impacted data to identify what information was involved and identify individuals to whom the data was related.

What did we do?
Promptly after the incident was detected on January 17, the SE Global Incident Response team was mobilized to respond to the attack, contain the incident, and to reinforce existing security measures, with the help of outside expertise. Critical resources were also taken offline as a preventive measure. The incident was contained and affected platforms were brought back online on January 31, 2024.

We worked as quickly as possible to identify and review the affected data and determine which employees and related individuals were affected so we could provide notice. While the dataset that was impacted was a small portion of the Sustainability Business' total data, the data was unstructured which increased the complexity of the review process and necessitated that rigorous analysis to review the documents for any personal information, quality check those materials, and associate that data with the correct individual.

While this type of review took time to carry out, we believe that it was the best way to ensure we have an accurate and comprehensive understanding of the affected data and the impact on employees and related individuals.

What Information Was Involved?
We completed our review and determined that some of your personal information was contained in the files including your name together with the following: **<Exposed Data Elements>**.

What You Can Do
We encourage you to review the additional information on **Transunion Single Bureau Credit Monitoring** including instructions on how to activate your complementary, 24-month membership, as follows:

Although we are not aware of any fraud or misuse of any personal information due to this incident, as a precaution and to address any potential concerns, we are offering you a complementary, 24-month membership of **Transunion Single Bureau Credit Monitoring**. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of

identity theft. **Transunion Single Bureau Credit Monitoring** is completely free to you and enrolling in this program will not hurt your credit score.

These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **<UniqueCode>.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age.

Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Please also review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or security freeze on your credit file.

For More Information. The security of your personal information is important to us, and we sincerely regret that this incident occurred. If you have any questions or need additional information about this incident, please email SB.privacy.notification@se.com. <Custom Field 1>

Should you have any questions regarding **Transunion Single Bureau Credit Monitoring**, have difficulty registering, or require additional support in relation to the **Transunion Single Bureau Credit Monitoring**, please contact Cyberscout at 1-833-647-0356.

Sincerely,

<Custom Field 2>
<Custom Field 3>

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 PO Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the
U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies — Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to vvvvw.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports,

contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. 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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-8085318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-7430023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

For Texas Residents: You may contact and obtain information from your state attorney general at:
Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identitytheft
or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.