EXHIBIT 1

By providing this notice, Solix does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of all the files potentially impacted to determine what information was present and to whom it related. On June 17, 2025, Solix finalized this review and determined that information related to Washington residents could be affected. The information potentially impacted by this incident includes name, Social Security number, date of birth, medical information, and health insurance information.

Notice to Washington Residents

On July 18, 2025, Solix provided written notice of this incident to one thousand two hundred fifty (1,250) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Solix also posted a notice of the incident on the homepage of its website and issued a nationwide media notice on July 18, 2025. The website and media notices are attached here as ***Exhibit B*** and ***Exhibit C***.

Other Steps Taken and To Be Taken

Upon discovering the event, Solix moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. Solix is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year through CyberScout, a TransUnion company, at no cost to the individuals.

Additionally, Solix is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Solix is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Solix is also notifying state regulators, as necessary.

EXHIBIT A

Solix, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

July 18, 2025

NOTICE OF SECURITY INCIDENT

Dear :

Solix, Inc. ("Solix") is writing to notify you of an incident that may have impacted your information. This letter provides details of the incident, our response, and steps you may take to help protect your information should you feel it is appropriate to do so.

What Happened? On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted accounts to assess what information was contained therein and to whom it related. On June 17, 2025, Solix finalized this review and determined that information related to you could be affected.

What Information Was Involved? The information potentially impacted by this incident includes your name and the following:

What We Are Doing. Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the event, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure the security of its email tenant, and conducted a comprehensive review of the information potentially affected. Solix also notified law enforcement and enhanced its existing security protocols.

As an added precaution, Solix is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment if changes occur to your credit file. A 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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Information regarding these services and instructions on how to enroll can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process as we are not permitted to enroll you in these services.

What You Can Do. Solix encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Solix also encourages you to enroll in the complimentary services being offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-833-380-8315 Monday through Friday from 8:00 am to 8:00 pm Est, excluding holidays. You may also write to Solix at 10 Lanidex Plaza, Parsippany, NJ 07054.

Sincerely,

Solix, Inc.

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring 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: . 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Solix is located at 10 Lanidex Plaza, Parsippany, NJ 07054.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. Solix is located at 10 Lanidex Plaza, Parsippany, NJ 07054.

EXHIBIT B

NOTICE OF DATA SECURITY INCIDENT

Solix, Inc. ("Solix") is providing notice of an incident that may have impacted the privacy of information related to certain individuals. While Solix is unaware of any actual or attempted misuse of information in relation to the incident, it is providing affected individuals with information about the incident and steps individuals may take to help protect their information should they wish to do so.

What Happened? On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted accounts to assess what information was contained therein and to whom it related. On June 17, Solix finalized this review, and identified who could have been affected and the categories of data impacted by this event.

What Information Was Involved? Solix determined the type of information potentially impacted by this incident varies by individual, but may include name, address, Social Security number, date of birth, tax identification number, driver's license or state identification number, financial account information, medical information, health insurance information, and username with password.

What We Are Doing. Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure the security of its email tenant, and conducted a comprehensive review of the information potentially affected.

Solix is also mailing notification letters to affected individuals for whom it has a postal address. If you did not receive a notice letter but would like to inquire as to whether you were impacted, you can call the number below.

What You Can Do. Solix encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and credit reports for any unauthorized or suspicious activity. Individuals can also review the *Steps Individuals Can Take to Help Protect Their Information* below for further guidance.

For More Information. We understand you may have questions about the incident that are not addressed in this notice. Representatives are available to assist you with questions regarding this incident, from 8:00 a.m. to 8:00 p.m. EST, Monday through Friday, excluding holidays. Please call the help line at 1-833-380-8315. You may also write to Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT THEIR INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a

consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Solix is located at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

EXHIBIT C

SOLIX, INC. PROVIDES NOTICE OF
DATA SECURITY INCIDENT

July 18, 2025 – Parsippany, New Jersey. Solix, Inc. ("Solix") is providing notice of an incident that may have impacted the privacy of information related to certain individuals.

On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted email accounts to assess what information was contained therein and to whom it related. Solix recently finalized this review and identified who could have been affected and the categories of data impacted by this event. The type of information potentially impacted by this incident varies by individual, but may include name, address, Social Security number, date of birth, tax identification number, driver's license or state identification number, financial account information, medical information, health insurance information, and username with password.

Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its email tenant, and conducted a comprehensive review of the information potentially affected. Solix is also mailing notification letters to affected individuals for whom it has a postal address. Solix encourages individuals to remain vigilant against incidents of identity theft and fraud.

Interested individuals may obtain additional information about the incident by visiting Solix's website at https://www.solixinc.com/wp-content/uploads/2025/07/solix-updated-website-notice-20250715.pdf. They may also write to Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

EXHIBIT 1

By providing this notice, Solix does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of all the files potentially impacted to determine what information was present and to whom it related. On June 17, 2025, Solix finalized this review and determined that information related to Washington residents could be affected. The information potentially impacted by this incident includes name, Social Security number, date of birth, medical information, and health insurance information.

Notice to Washington Residents

On July 18, 2025, Solix provided written notice of this incident to one thousand two hundred fifty (1,250) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Solix also posted a notice of the incident on the homepage of its website and issued a nationwide media notice on July 18, 2025. The website and media notices are attached here as ***Exhibit B*** and ***Exhibit C***.

Other Steps Taken and To Be Taken

Upon discovering the event, Solix moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. Solix is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year through CyberScout, a TransUnion company, at no cost to the individuals.

Additionally, Solix is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Solix is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Solix is also notifying state regulators, as necessary.

EXHIBIT A

Solix, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

July 18, 2025

NOTICE OF SECURITY INCIDENT

Dear :

Solix, Inc. ("Solix") is writing to notify you of an incident that may have impacted your information. This letter provides details of the incident, our response, and steps you may take to help protect your information should you feel it is appropriate to do so.

What Happened? On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted accounts to assess what information was contained therein and to whom it related. On June 17, 2025, Solix finalized this review and determined that information related to you could be affected.

What Information Was Involved? The information potentially impacted by this incident includes your name and the following:

What We Are Doing. Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the event, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure the security of its email tenant, and conducted a comprehensive review of the information potentially affected. Solix also notified law enforcement and enhanced its existing security protocols.

As an added precaution, Solix is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment if changes occur to your credit file. A 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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Information regarding these services and instructions on how to enroll can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process as we are not permitted to enroll you in these services.

What You Can Do. Solix encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Solix also encourages you to enroll in the complimentary services being offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-833-380-8315 Monday through Friday from 8:00 am to 8:00 pm Est, excluding holidays. You may also write to Solix at 10 Lanidex Plaza, Parsippany, NJ 07054.

Sincerely,

Solix, Inc.

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring 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: . 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Solix is located at 10 Lanidex Plaza, Parsippany, NJ 07054.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. Solix is located at 10 Lanidex Plaza, Parsippany, NJ 07054.

EXHIBIT B

NOTICE OF DATA SECURITY INCIDENT

Solix, Inc. ("Solix") is providing notice of an incident that may have impacted the privacy of information related to certain individuals. While Solix is unaware of any actual or attempted misuse of information in relation to the incident, it is providing affected individuals with information about the incident and steps individuals may take to help protect their information should they wish to do so.

What Happened? On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted accounts to assess what information was contained therein and to whom it related. On June 17, Solix finalized this review, and identified who could have been affected and the categories of data impacted by this event.

What Information Was Involved? Solix determined the type of information potentially impacted by this incident varies by individual, but may include name, address, Social Security number, date of birth, tax identification number, driver's license or state identification number, financial account information, medical information, health insurance information, and username with password.

What We Are Doing. Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure the security of its email tenant, and conducted a comprehensive review of the information potentially affected.

Solix is also mailing notification letters to affected individuals for whom it has a postal address. If you did not receive a notice letter but would like to inquire as to whether you were impacted, you can call the number below.

What You Can Do. Solix encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and credit reports for any unauthorized or suspicious activity. Individuals can also review the *Steps Individuals Can Take to Help Protect Their Information* below for further guidance.

For More Information. We understand you may have questions about the incident that are not addressed in this notice. Representatives are available to assist you with questions regarding this incident, from 8:00 a.m. to 8:00 p.m. EST, Monday through Friday, excluding holidays. Please call the help line at 1-833-380-8315. You may also write to Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT THEIR INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a

consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Solix is located at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.

EXHIBIT C

SOLIX, INC. PROVIDES NOTICE OF
DATA SECURITY INCIDENT

July 18, 2025 – Parsippany, New Jersey. Solix, Inc. ("Solix") is providing notice of an incident that may have impacted the privacy of information related to certain individuals.

On March 24, 2025, Solix was alerted to suspicious activity in certain employee email accounts. Solix immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email accounts of several Solix employees from March 24 to March 27, 2025. Thereafter, Solix undertook a comprehensive review of the impacted email accounts to assess what information was contained therein and to whom it related. Solix recently finalized this review and identified who could have been affected and the categories of data impacted by this event. The type of information potentially impacted by this incident varies by individual, but may include name, address, Social Security number, date of birth, tax identification number, driver's license or state identification number, financial account information, medical information, health insurance information, and username with password.

Solix takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, Solix conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its email tenant, and conducted a comprehensive review of the information potentially affected. Solix is also mailing notification letters to affected individuals for whom it has a postal address. Solix encourages individuals to remain vigilant against incidents of identity theft and fraud.

Interested individuals may obtain additional information about the incident by visiting Solix's website at https://www.solixinc.com/wp-content/uploads/2025/07/solix-updated-website-notice-20250715.pdf. They may also write to Solix at 10 Lanidex Plaza, Parsippany, New Jersey 07054.