April __, 2026

Subject: Notice of Data Breach

Dear Isabelle Guilbeault,

Solotech Inc. ("**Solotech**" or "**we**") places great importance on its employees and partners and understands the need to protect your personal information. We are writing to inform you about a recent cybersecurity incident that affected Solotech's computer systems and may involve some of your personal information. Your security and protection of your personal information are of utmost importance to us. Accordingly, we want to provide you with information about what happened and what we are doing about it.

WHAT HAPPENED?

On March 31, 2026, we became aware that an unauthorized third party gained access to some of our computer systems ("**Incident**").

WHAT INFORMATION WAS INVOLVED?

The unauthorized third party may have accessed personal information that you may have provided to us in connection with your relationship with Solotech, such as your full name, contact information, date of birth, a government-issued ID (e.g., driver's license, passport, Social Security Number, or other tax identification numbers), details related to the bank account used for direct deposits, and other general information (e.g., compensation, insurance claims, and drug tests).

WHAT WE ARE DOING

As soon as we became aware of the Incident, we took immediate steps to investigate and remediate the situation to minimize any potential risk to you. While the precise start date of the incident remains under investigation, we currently estimate that the unauthorized access likely occurred between March 30-31, 2026.

That unauthorized access has now been disabled by our IT experts. We also conducted a thorough review of the potentially affected systems and implemented additional security measures to protect them. To date, our investigation has not revealed any evidence of misuse of any personal information, but we have not been able to rule out the possibility

that the third party accessed or took copies of your personal information during this period of incident. Solotech is working closely with law enforcement to ensure the incident is properly addressed.

WHAT YOU CAN DO

We recommend that you review the section below entitled **Steps You Can Take to Better Protect Your Information** for more information on measures you can take to protect yourself. We also recommend increasing your monitoring of any suspicious activity or transactions involving your personal information.

We have retained the assistance of **Equifax** and arranged a **two-year** subscription to **Equifax Credit Watch Gold** an online credit monitoring and identity restoration service. A description of this product and enrollment instructions are provided below. You must complete the enrollment process by **July 31, 2026**. We recommend that you consider enrolling, as these services are provided to you free of charge by Solotech.

We deeply regret any inconvenience this incident may cause you. If you have any further questions, please contact us at **infocyber@solotech.com** or call us at 866-992-9466.

Sincerely,

Isabelle Guilbeault
Privacy Officer and Vice President, Legal Affairs

Steps You Can Take to Better Protect Your Information

Review Your Account Statements and Report Suspicious Activity to Law Enforcement

We recommend you remain vigilant by reviewing your account statements and monitoring your credit reports for any signs of fraud or identity theft. If you detect any suspicious activity or errors on an account, promptly notify the financial institution or other business at which you maintain your account. We recommend that you promptly report any fraudulent activity or any suspected identity theft to law enforcement authorities, including your state attorney general, law enforcement, and the Federal Trade Commission ("FTC"). To file a complaint with the FTC, please visit IdentityTheft.gov or call 877-ID-THEFT (877-438-4338).

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from at least one 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 Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the printable request form at https://www.annualcreditreport.com/manualRequestForm.action or fill out the online form at https://www.annualcreditreport.com/requestReport/landingPage.action. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

	Equifax	**Experian**	**TransUnion**
Contact Information	(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19016

Consider Placing a Fraud Alert or Credit Freeze on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, free of charge, 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 credit 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 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency filed by you concerning identity theft if you are a victim of identity theft.

If you wish to place a fraud alert or credit freeze on your credit report, please contact the three major credit reporting bureaus or the FTC for more information.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the FTC's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. You may contact the Federal Trade Commission for more information on fraud alerts, credit freezes, and how to protect yourself from identity theft at: 600 Pennsylvania Avenue NW, Washington, DC 20580, at www.identitytheft.gov, or by calling 877-ID-THEFT (877-438-4338) or TTY: 866-653-4261. You can also contact your state's attorney general for more information on preventing or avoiding identity theft:

- For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.
- For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, 502-696-5300.
- For Massachusetts residents, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain more information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 617-727-2200, https://www.mass.gov/contact-the-attorney-generals-office.
- For New Mexico residents, you have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or https://www.ftc.gov.

- For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, https://www.ag.ny.gov, 800-771-7755. You may also contact the New York Bureau of Internet and Technology at 28 Liberty Street, New York, NY 10005, http://www.dos.ny.gov/consumerprotection, 212-416-8433.
- For North Carolina residents, the North Carolina Attorney General can be contacted at Consumer Protection Division, Mail Service Center 9001, Raleigh, NC 27699, https://ncdoj.gov/, 877-566-7226.
- For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, https://www.doj.state.or.us, 503-378-4400.

Isabelle Guilbeault
Activation Code: **#########**
Enrollment Deadline: **31 July 2026**

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 **#########** 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.