



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[NAME]
[ADDRESS]
[CITY] [STATE] [ZIP]

February 24, 2023

Dear [Name]:

On February 3, 2023, we sent you a notice informing you that SOMACIS Inc. suffered a security incident that resulted in the exfiltration of employee data from our systems. Since then, the Company has been working with a third-party cybersecurity firm to determine the scope of the security incident and identify the potentially exfiltrated data. Although the forensic investigation is ongoing and we do not yet have all the answers, we felt it important to inform you of the information that we have gathered about the incident, and let you know the steps that we are taking to address it.

What Happened?

On January 13, 2023, we discovered that a bad actor had remotely logged-in to a SOMACIS' server. The bad actor was attempting to encrypt the Company's servers to carry out a ransomware attack. Due to the swift actions of our IT lead, the bad actor was unable to carry out their plan and the Company's systems were not encrypted. Following the attempted attack, the Company performed a thorough review of our network perimeter to ensure that the Company was safe from further attack. In addition, we began performing a thorough review of our systems as part of our investigation into the bad actor's potential actions while on our server. Unfortunately, on January 26, 2023, we learned that the bad actor had been able to exfiltrate a subset of our data during the January 13 attempted attack.

What Information Was Involved?

As stated at the outset of the letter, the forensic investigation into the scope of the impacted data is ongoing, and so we cannot at this point definitively state the data that may have been exfiltrated. However, we believe it is possible that the bad actor may have obtained your name and Social Security number.

What We Are Doing

Out of an abundance of caution, the Company is offering you two years of identity protection services, at no cost to you, through Experian, one of the three nationwide credit bureaus. Your two-year membership in Experian's IdentityWorksSM product provides identity restoration services, fraud detection tools, dark web surveillance, and other benefits, which include monitoring your credit file at Experian.

Starting today, you can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until May 31, 2025 by calling Experian at 1-877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate the fraud detection tools available through IdentityWorks. This product provides you with identity detection, credit monitoring, and resolution of identity theft.

What You Can Do

If you wish to enroll in IdentityWorks, you will need to do the following:

1. **Visit** the IdentityWorks web site: <https://www.experianidworks.com/plus> or call 1-877-890-9332 to enroll and provide Engagement Number **[NUMBER]**.
2. **Provide** your Activation Code: **[CODE]**.

Enrollment Deadline: May 31, 2023 (your Activation Code will not work after this date).

If you have any questions concerning IdentityWorks, or if you prefer to enroll over the phone for delivery of your membership via US mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number **[NUMBER]** as proof of eligibility for the identity protection product by Experian.

Other Important Information

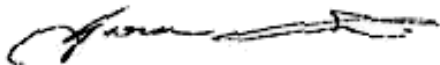
In addition to the offer of IdentityWorks, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

Please be assured that the Company takes seriously both the security of your personal information and this incident, and we have taken appropriate steps to prevent a recurrence. We have also reported this incident to the FBI and we are cooperating with its investigation. We have not delayed notifying you at the request of law enforcement.

For More Information

The Company regrets this incident and any inconvenience it may cause you. Should you have any questions or concerns regarding this incident, please do not hesitate to contact our call center at (888) 935-7074 between 6 A.M./9 A.M. and 2 P.M./5 P.M (PT/ET), Monday through Friday.

Sincerely,



Giovanni Tridenti
CEO
SOMACIS Inc.

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorks. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks membership. Experian's IdentityWorks product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only¹.
- **Credit Monitoring:** Actively monitors your credit files at Experian for indicators of fraud.
- **Dark Web Surveillance:** Daily scans of over 600,000 web pages to detect if your information is stolen.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorks membership expires.
- **\$1 Million Identity Theft Insurance**²: Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks product to Experian. A credit card is not required for enrollment in IdentityWorks. Enrollment in IdentityWorks will not affect your credit score. The Terms and Conditions for this offer are located at: www.ExperianIDWorks.com/restoration.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled to one free copy of your credit report from each of the three national credit bureaus every 12 months. Until December 31, 2023, however, you are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. Errors in this information may be signs of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorks identity resolution agent toll-free at 1-877-890-9332 or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to the Company, your local police department, your state's attorney general, and the Federal Trade Commission.

5. You have the right to place a "security freeze" on your credit report. A security freeze will prohibit a credit bureau from releasing information in your credit file without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please understand that placing a security freeze on your credit file may delay, interfere with, or prevent the timely approval of any subsequent request or application you make for a new loan, mortgage, or any other account involving the extension of credit.

¹Offline members will be eligible to call for additional reports quarterly after enrolling.

²The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

To place a security freeze on your credit file, contact the three nationwide credit bureaus, listed below. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. There is no charge to place a security freeze.

The contact information for all three credit bureaus is as follows:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that credit bureau processes your fraud alert, it will notify the other two, which then must also place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; <http://www.ftc.gov/idtheft/>; (877) IDTHEFT (438-4338).

Massachusetts Residents: Massachusetts law gives you the right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of filing.

New York Residents: You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
www.ag.ny.gov