

SAMPLE NOTICE LETTER

[Date]

[First Name Last Name]

[Address]

[City, State Zip]

RE: Notice of Security Incident

Dear [First Name],

Naegle Communications and its affiliated businesses (“Company”, “we” or “our”) takes the security and protection of your personal information seriously. This letter is in regard to an incident that the Company experienced involving the security of your personal data on one of its systems. We sincerely regret to inform you that the incident may have resulted in the unauthorized access or viewing of your personal information (“Incident”). Once aware of the Incident, the Company quickly took steps to eliminate the threat of further unauthorized access, safeguarded the information in its possession, and conducted an investigation. We are providing this letter to you out of an abundance of caution, in accordance with applicable law, and to provide you information about the Incident and what you can do to remain vigilant and protect your personal information.

What Happened

On or about July 22, 2025, the Company became aware of unauthorized access to a single Company server on which various employee files were maintained along with other Company records. Based on our investigation, the threat actor was able to view and possibly remove certain files from this server. Some of these files included records related to current and former Company employees. Once aware of the unauthorized access, the Company immediately secured the affected server, and any files contained on the server. The Company then commenced a thorough investigation of the underlying root causes and scope of the Incident.

What Information Was Involved

Based on our investigation, the files at risk were comprised of various records required for Company compliance and general operations, including certain current and former employee files and business partners. Not every employee or individual has information at risk because of this Incident and not every file contained the same records or personal information. However, we can confirm files may have contained an individual’s first and last name, home address, Social Security number and date of birth. In some instances, the files also included the routing number and account number for any bank account which individuals would have had Company payroll or funds deposited.

What We Are Doing

Once aware of the Incident, we immediately removed the affected server from our network and took steps to identify and remediate any potential threats to the server and our Company network. We were able to safely restore any Company files impacted by the Incident. We have also notified law enforcement. The Company has implemented various changes to further secure these files and the Company's information systems against the potential recurrence of a similar incident.

As a resident of Massachusetts, are you also entitled to credit monitoring services. We have provided a complimentary registration for such services with Experian. Please follow the instructions below on how to enroll at no charge.

What You Can Do

Our investigation has only identified Company files that may be at risk because of this Incident. As of now, we have no evidence or reports of the misuse of any Company employee information as a result of this Incident. Regardless, as always, you should remain vigilant for any potential misuse of your personal information. We have provided additional information below on ways you can remain diligent and protect your personal information.

If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information

You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites. In some cases, fees may apply.

Equifax - 1-888-766-0008
P.O. Box 740256
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/>

Experian - 1-888-397-3742
P.O. Box 4500
Allen, TX 75013
<https://www.experian.com/help/>

Trans Union - 1-800-916-8800
P.O. Box 2000
Chester, PA 19022
<https://www.transunion.com/credit-help>

Credit Reports. You can request credit reports from all three credit bureaus be sent to you free of charge. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Security Freeze. Under state law, a security freeze (or a credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

1. Your full name;
2. Social Security number;
3. Date of birth;
4. Mobile number;
5. Current postal address;
6. Email address; and
7. Any other information that the Credit Bureau may require.

The credit bureaus have one (1) business day after your request to place a security freeze, if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three (3) business days. The credit bureaus must also send written confirmation to you within five (5) business days.

In order to lift the security freeze to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one (1) hour. If you request the thaw by regular mail, the credit bureaus have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find

additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC by using the information below.

Federal Trade Commission - 1-202-326-2222 or 877-FTC-HELP.
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at:

Contact: Naegele Communications
Email: contactNCI@naegelenet.com
Telephone: 612-449-2757
Address: Naegele Communications
5201 Eden Ave. Suite 300
Edina, MN 55436

Sincerely,

Cynthia Schneider
Naegele Communications

Experian Identity Restoration and Credit Monitoring Services

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

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

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

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

- Ensure that you **enroll by December 31, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
- Provide your **activation code**:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 931-7577. by December 31, 2025. Be prepared to provide engagement number [#] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** The 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.