

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

NCH Corporation ("NCH") understands the importance of protecting information. We are writing to inform you, on our behalf and on behalf of certain current and former affiliates, that we recently identified and addressed an incident involving some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps that you can consider taking.

Who Are We, and Why Do We Have Your Information?
We are a company that provides industrial maintenance, water treatment, and hygiene solutions. We have your information because you are a current or former employee, the dependent or beneficiary of a current or former employee, or for another business-related reason.

What Happened?
On March 9, 2026, we became aware that an unauthorized actor may have taken files from our network. We immediately implemented our response procedures, took containment measures, and launched an investigation with the support of third-party cybersecurity professionals. We also notified law enforcement and are supporting its investigation.

The evidence showed that there was unauthorized activity in our network between January 21, 2026, and February 25, 2026. During that time, an unauthorized actor obtained copies of certain files from our network. We completed our review of the files involved on October 2, 2026, and determined that one or more of the files contained your information.

What Information Was Involved?
The files included your name, Social Security number, taxpayer identification number, driver's license number, and/or state identification card number. The files also may have included one or more of the following: passport number, other government-issued identification number, financial account information, payment card information, medical information, and/or health insurance information.

What We Are Doing.
We wanted to notify you of this incident and to assure you that we take it seriously. We have arranged for you to receive a complimentary <<CM Duration>> in IDX's identity protection service. This service helps detect possible misuse of your information and provides you with identity protection support focused on identification and resolution of identity theft.

Additionally, to help prevent something like this from happening again, we have taken steps to enhance our existing security measures.

What You Can Do.
It is always advisable to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant financial institution or credit bureau immediately. Additionally, we encourage you to enroll in the complimentary identity protection service we are making available to you through IDX. If you enrolled in the service when we offered it in November and December 2025, you do not need to re-enroll. We are automatically extending the duration of the membership for you. If you did not previously enroll, you can enroll by following the instructions on the next page. You will also find additional information about the IDX identity protection service and identity theft prevention on the pages that follow this letter.

For More Information.
We regret that this incident occurred and apologize for any inconvenience. If you have any questions, please call 888-504-8648, Monday through Friday, between 9 a.m. and 9 p.m. ET.

Sincerely,

NCH Corporation

Enrolling in IDX Identity Protection Services

We are offering you identity theft protection services through IDX. As explained in further detail below, the IDX identity protection services include <<CM Duration>> of credit and CyberScan monitoring; a $1,000,000 insurance reimbursement policy; and fully managed identity theft recovery services.

1. **Website and Enrollment.** We encourage you to enroll in the free IDX identity protection services by scanning the QR code at the bottom of this document or going to https://app.idx.us/account-creation/protect. Please use the following Enrollment Code to enroll: <<ACTIVATION CODE>>. Please note the deadline for enrolling is <<ENROLLMENT DEADLINE>>. Once you enroll, you and your family will have access to the following services:

- **SINGLE BUREAU CREDIT MONITORING** (Adults*). Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect a member's credit record.
- **CYBERSCAN**™. Monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, medical ID numbers, and other unique identifiers.
- **IDENTITY THEFT INSURANCE**. Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
- **FULLY MANAGED IDENTITY RECOVERY** – IDX's fully managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring services included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Review your credit reports. If you discover any suspicious items and have enrolled in the IDX identity protection services, notify them immediately by calling (866) 329-9984 or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's IDCare team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an IDCare Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

4. Questions? If you have questions regarding the IDX services or need assistance enrolling, please call (866) 329-9984. ***Please note***, a separate call center has been established to answer your questions about the incident.

Enrollment Code: <<ACTIVATION CODE>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once per week from each of the three nationwide credit reporting companies. To order your weekly free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. 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.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

NCH Corporation may be contacted by mail at 2727 Chemsearch Boulevard, Irving, Texas 75062 or by telephone at (800) 527-9919.

Protecting Health Insurance or Medical Information: It is always advisable to review any statements you may receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, contact your insurer or provider immediately.