

APPENDIX

NCH Corporation (“NCH”) and many organizations use Oracle’s E-Business Suite (“EBS”) software to help manage their operations. In August 2025, an unauthorized actor leveraged a previously unknown vulnerability in Oracle EBS to take information from numerous organizations’ Oracle EBS applications. NCH recently learned that it was one of those organizations.

Upon becoming aware of the incident, NCH immediately implemented its response procedures, took measures to secure its implementation of Oracle EBS, and launched an investigation with the support of third-party cybersecurity professionals. NCH also notified law enforcement and is supporting its investigation.

The evidence showed that an unauthorized actor obtained files from the NCH Oracle EBS application in mid-August 2025. NCH reviewed the files and, on November 25, 2025, determined that one or more of the files contained the names and Social Security numbers of approximately 13 Nebraska residents.

Today, December 5, 2025, NCH is mailing notification letters via First-Class mail to the Nebraska residents. A copy of the notification letter template is enclosed. NCH is offering individuals a complimentary, one-year membership to credit monitoring and identity protection services. NCH also has established a dedicated, toll-free call center that individuals can call to obtain more information regarding the incident.

To help prevent something like this from happening again, NCH applied the patch that Oracle developed for Oracle EBS after the vulnerability was discovered and took other measures to secure its Oracle EBS instance.



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>>

Dear <<Full Name>>,

NCH Corporation (“NCH”) understands the importance of protecting information. We are writing to inform you 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?

NCH and many organizations use Oracle’s E-Business Suite (“EBS”) software to help manage their operations. An unauthorized actor leveraged a previously unknown vulnerability in Oracle EBS to take information from numerous organizations’ Oracle EBS applications. We recently learned that NCH was one of those organizations.

Upon becoming aware of the incident, we immediately implemented our response procedures, took measures to secure our implementation of Oracle EBS, 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 an unauthorized actor obtained files from our Oracle EBS application in mid-August 2025. We reviewed the files and, on November 25, 2025, determined that one or more of the files contained your information.

What Information Was Involved?

The information included your name and one or more of the following: date of birth, Social Security number, and benefits enrollment 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 one-year membership to 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 applied the patch that Oracle developed for Oracle EBS after the vulnerability was discovered and took other measures to secure our Oracle EBS instance.

What You Can Do.

We encourage you to enroll in the complimentary identity protection service we are making available to you through IDX. For more information on identity theft prevention and instructions on how to activate your complimentary membership, please review the additional information provided in this letter.

For More Information.

We regret that this incident occurred and apologize for any inconvenience. If you have any questions, please call 888-360-9934, Monday through Friday, between 9:00 a.m. and 9:00 p.m. EST.

Sincerely,

NCH Corporation

Enrolling in IDX Identity Protection Services

We are offering you and your family (2 adults and up to 5 minors) identity theft protection services through IDX. As explained in further detail below, the IDX identity protection services include 12 months 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: **ZK5A8S3FW**. Please note the deadline for enrolling is **March 26, 2026**. 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 **(833) 788-9712** 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 (833) 788-9712. **Please note**, a separate call center has been established to answer your questions about the incident.

Enrollment Code: **ZK5A8S3FW**

To Enroll, Scan the QR Code Below:



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 every 12 months from each of the three nationwide credit reporting companies. To order your annual 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.

Additional Information for Residents of the Following States

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: This incident involves <<Rhode Island Count>> individuals in Rhode Island. Under Rhode Island law, 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 information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.