Richard Halm
T (312)985-5564
F (312)985-5952
Email:rhalm@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

July 8, 2026

VIA PORTAL

Nebraska Attorney General
2115 State Capitol
Lincoln, NE 68509

Dear Attorney General Hilgers,

We represent First National Holdings, LLC ("First National") with respect to a data security incident involving personal information as described below. First National takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On or around February 9, 2026, First National discovered suspicious activity that limited access to certain computer systems. First National immediately implemented its incident response protocols, took steps to secure and contain the incident, and engaged external cybersecurity experts to assist with an investigation. On April 1, 2026, the investigation determined that some files may have been accessed by an unauthorized individual. First National conducted a thorough review of the files at issue, and on May 29, 2026, determined that the unauthorized individual may have accessed personal information during the incident.

Impacted information included names and Social Security numbers.

2. Number of residents affected

Two (2) Nebraska residents were notified of the incident. Potentially impacted individuals were notified beginning July 8, 2026. A copy of the form notification letter is enclosed as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, First National has restored its systems, tightened access controls, and implemented additional technical safeguards to strengthen the security of their systems, among other measures. Additionally, letters were mailed to potentially affected individuals, which included instructions for enrolling in twelve (12) months of credit monitoring and identity protection services through IDX at no cost.

4. Contact information

First National takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at rhalm@clarkhill.com or (312) 985-5564.

Sincerely,

CLARK HILL

Richard Halm

Richard Halm
Member

cc: Lauren M. Williams – lmwilliams@clarkhill.com

EXHIBIT A

First National Holdings, LLC
Return to IDX
P.O. Box 1907
Suwanee, GA 30024

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: October 8, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

July 8, 2026

NOTICE OF DATA SECURITY <<INCIDENT/BREACH>>

Dear <<First Name>> <<Last Name>>,

First National Holdings, LLC experienced a data security incident that may have impacted some of your personal information. We take the privacy and security of our information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On February 9, 2026, we experienced a cybersecurity incident that limited access to certain computer systems. In response, we initiated our incident response protocols, took steps to secure and contain the incident, and engaged cybersecurity experts to assist with an investigation. On April 1, 2026, we determined that some files belonging to a limited number of individuals may have been accessed by an unauthorized individual. On May 29, 2026, we determined that your personal information was potentially present within these files.

What Information Was Involved?

The potentially impacted information includes your name, <<data elements>>. While we do not have any evidence that this information has been misused, we are informing individuals about this incident out of an abundance of caution.

What We Are Doing

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have worked to restore our systems, tightened our access controls, and are evaluating additional technical safeguards to strengthen the security of our systems. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-855-758-9690, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

If you have questions, please call 1-855-758-9690 Monday through Friday from 9 am - 9 pm Eastern Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

First National Holdings, LLC

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is October 8, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring 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. Telephone. Contact IDX at 1-855-758-9690 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling 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 our ID Care 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 ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, https://oag.maryland.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.