LEPANT LAW OFFICE, PC, LLO
SCHWAB & LEPANT

DAVID P. LEPANT
COLE A. BODFIELD*

RONALD L. SCHWAB, *Retired*

119 N 5TH ST | BEATRICE, NE 68310 lawoffice@lepantlaw.com PHONE: (402) 223-4071

311 5TH ST | FAIRBURY, NE 68352 www.lepantlaw.com PHONE: (402) 729-3368

*Cole A. Bodfield is licensed in Nebraska and Kansas

[redacted]

May 8, 2025

RE: Notification of Data Breach

Dear [redacted]

Lepant Law Office, P.C., L.L.O. (the "firm", or "we"), takes the privacy and confidentiality of your information very seriously. We are writing to inform you of a recent data security incident that may have affected your personal information. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected individuals about the incident, and about tools you can use to protect yourself against possible identity theft or fraud.

<u>What Happened?</u>

On March 5, 2025, at 6:56 AM, we were notified via our information technology vendor that an unauthorized bad actor gained access to a firm server and infected such server with ransomware. This resulted in the bad actor gaining access to personal data on such server. We took quick actions to mitigate the situation and were able to disconnect the infected server and remove the bad actor's access to the firm's systems by approximately 8:30 AM on the same day. Our investigation into the matter is ongoing, but we wanted to provide you with information about what happened and the next steps we are taking to address the situation.

<u>What Information Was Involved?</u>

The information that may have been accessed about you includes first and last names, addresses, Social Security Numbers, and drivers' license numbers.

<u>What Are We Doing?</u>

Upon discovering this incident, we took immediate action and began an investigation to confirm what information and systems were impacted. We are working closely with our information technology vendor and insurance provider to understand the full scope of the incident and to enhance our security measures to prevent similar incidents from occurring in the future. In fact, we have implemented a number of security measures to help prevent any future incidents and to restore the security of our systems and the confidentiality of information we handle.

What Can You Do?

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information. The attachment provides precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, obtaining a free credit report, and enrolling in free identity theft monitoring. Additionally, you should remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Once again, we deeply regret any inconvenience this may have caused and appreciate your understanding as we work diligently to address this issue.

If you have any questions or concerns, please do not hesitate to contact our team at **(402) 223-4071**.

Sincerely,

Cole A. Bodfield

Lepant Law Office, P.C., L.L.O

Steps You Can Take to Further Protect Your Information

Consider Placing a Fraud Alert on Your Credit File

You may place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

Consider Placing a Security Freeze on your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (800) 349-9960 (888) 298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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. Using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your local law enforcement agency to file a police report, the state attorney general and the Federal Trade Commission. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts

You may also file a complaint with the FTC by contacting them on the web at IdentityTheft.gov, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

We recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.