

EXHIBIT 1

This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Moore, Clarke, DuVall & Rodgers (“MCDR”) does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

In late May of last year, MCDR was alerted to potential suspicious activity within its computer network. MCDR promptly launched an investigation, with the assistance of third-party cybersecurity and digital forensics specialists, and determined it was the victim of a sophisticated cyberattack. MCDR worked quickly to secure its systems and investigate whether this event resulted in any impact to information. MCDR also promptly reported this event to federal law enforcement and supported their investigation. Through the investigation, MCDR determined that an unauthorized actor had the ability to access certain files within an MCDR system between May 17, 2024, and May 30, 2024, and certain data on those systems was viewed and downloaded. MCDR subsequently worked with third-party specialists to undertake a comprehensive review of the impacted files to determine what data they contained and to whom it related. Following the third-party review, MCDR undertook a manual review of the records to identify address information for notifications.

While the review was ongoing, MCDR provided an initial wave of notice on April 16, 2025 to potentially affected individuals. Since then, MCDR continued to review its records to identify additional address information to provide notice of this event. This additional review recently completed and MCDR identified Nebraska residents in scope for notice.

The personal information that could have been subject to unauthorized access for Nebraska residents includes: name and Social Security number.

Notice to Nebraska Residents

On August 11, 2025, MCDR continued providing written notice of this event to potentially affected individuals, including approximately two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, MCDR moved quickly to investigate and respond, assess the security of its computer systems, and identify potentially affected individuals. Further, MCDR reported the event to federal law enforcement. MCDR is also working to implement additional cybersecurity safeguards and training to its employees. As a precaution, MCDR is providing access to credit monitoring and identity restoration services for twelve (12) months, through IDX, to potentially affected individuals at no cost to these individuals.

Additionally, MCDR is providing notified individuals with guidance on how to better protect against identity theft and fraud. MCDR is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

MCDR provided written notice of this event to appropriate state regulators and the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXXXX>>
Enrollment Deadline: November 11, 2025

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 11, 2025

<<CA ONLY: Notice of Data Breach>>

Dear <<Name 1>> <<Name 2>>:

Moore, Clarke, DuVall & Rodgers (“MCDR”) is writing to make you aware of a recent event involving certain information related to you. This letter includes information about the event, our response to it, and steps you may take to help protect your information should you determine it is appropriate to do so.

What Happened? In late May of last year, MCDR was alerted to potential suspicious activity within our firm’s computer systems. We promptly launched an investigation to identify the nature and scope of the matter and worked quickly to secure our systems. We worked with cybersecurity specialists to determine whether this event resulted in any impact to information housed on our systems. We also promptly reported this event to federal law enforcement and supported their investigation. Through our investigation, we determined that an unauthorized party had the ability to access certain files within MCDR’s system between May 17, 2024, and May 30, 2024, and certain data on those systems was viewed and downloaded. We subsequently worked with third-party specialists to undertake a comprehensive review of the impacted files to determine what data they contained and to whom it related. Following the third-party review, we undertook a manual review of the records to identify address information for notifications. We recently completed our review.

What Information Was Involved? Our investigation determined that at the time of the event, your name and <<IMPACTED DATA ELEMENTS>> were stored within the impacted system.

What We Are Doing. We take this event and information security seriously. Upon learning of the activity, we quickly took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further enhance our information security posture.

As an additional precaution, MCDR is offering you access to <<12/24>> months of complimentary credit monitoring and identity restoration services through IDX. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed document, *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. For additional questions, please contact our toll-free assistance line at 1-800-939-4170. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 11, 2025. You can also write to MCDR at 2829 Old Dawson Road Albany, GA 31707.

Sincerely,

Moore, Clarke, DuVall & Rodgers

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

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.

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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12244-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.