

EXHIBIT 1

By providing this notice, The Browning Group 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.

The Browning Group identified unusual email activity and undertook an investigation to determine the nature and scope of the issue. Through the investigation, it determined certain email accounts were subject to unauthorized access in October and November 2024. The Browning Group undertook a review to confirm what information may have been present in the account. Out of an abundance of caution, The Browning Group is notifying individuals whose information may have been present in the accounts during the time of unauthorized access. While the investigation has not confirmed the precise information that was in the relevant email accounts, the types of data that may have been present would include personal information such as name, Social Security number, and financial account information. On or about May 21, 2025, The Browning Group provided written notice of this incident to two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

In response to this incident, The Browning Group conducted a thorough investigation to confirm the full nature and scope of the event. The Browning Group is also working to implement additional safeguards and training to its employees. The Browning Group is also providing potentially affected individuals access to credit monitoring services for twelve (12) months through IDX. Additionally, The Browning Group is providing impacted individuals with guidance on how to better protect against identity theft and fraud, as demonstrated in the notice letter attached here as ***Exhibit A***. The Browning Group is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A



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

<<Name 1>> <<Name 2>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<< Variable Data 1>>

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

We are writing to make you aware of an incident that may affect some of your personal information. This notice includes information about the incident, steps taken in response, and resources available to help you protect your information, should you feel it is appropriate to do so.

What Happened? We identified unusual email activity and undertook an investigation to determine the nature and scope of the issue. Through the investigation, we determined certain email accounts were subject to unauthorized access in October and November 2024. We undertook a review to confirm what information may have been present in the account. <<Variable Data 2>> Out of an abundance of caution, we are notifying individuals whose information may have been present in the accounts during the time of unauthorized access.

What Information Was Involved? While we have not confirmed that your information was in the relevant email accounts, the types of data that may have been present would include personal information such as name, Social Security number, and financial account information.

What We Are Doing. In response to this incident, steps were taken to secure the relevant email accounts and an investigation was conducted to confirm the nature and scope of the incident. We are now notifying those who may be affected and, as an added precaution, we are providing you with access to [REDACTED] months of credit monitoring and identity protection services, through IDX, at no cost to you. Directions on how to enroll in these services, as well as more information on other steps you can take to protect information, are provided in the attached *Steps Individuals Can Take To Help Protect Personal Information*. We encourage you to enroll in these complimentary services, as we are unable to enroll on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and activity for at least the next 12 to 24 months and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the attached *Steps Individuals Can Take To Help Protect Personal Information* section of this letter.

For More Information. If you have additional questions, please contact our dedicated assistance line at [REDACTED], Monday through Friday from 8:00 am – 8:00 pm Central (excluding major U.S. holidays). You may also write to us at 2 Inverness Drive, Suite 187, Englewood, CO 80112.

Sincerely,
The Browning Group II, LLC

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

STEPS INDIVIDUALS 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 [REDACTED] 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 1-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/credit-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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.