EXHIBIT 1

We represent PrimeLending, a PlainsCapital Company ("PrimeLending"), located at 18111 Preston Road, Suite 900, Dallas, TX 75252. We write to notify your Office of a third-party data security event. Please note, this incident did not happen within and/or affect PrimeLending's network or IT systems. By providing this notice, PrimeLending does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around July 24, 2023, PrimeLending received notice from PrimeLending's parent company, PlainsCapital Bank ("PlainsCapital" or the "Bank"), that certain PrimeLending information was impacted by a global cyberattack conducted against MOVEit, a file transfer software used by one of the Bank's third-party vendors (the "Vendor") and deployed by many government agencies, enterprise corporations, and leading technology and professional service organizations world-wide. A large number of these organizations globally have been impacted by this zero-day cyberattack. Neither PrimeLending nor PlainsCapital directly engages with MOVEit; however, PlainsCapital's third-party vendor, a leading financial technology service provider, utilizes the MOVEit software to deliver information associated with contracted information processing services, and was impacted by the incident. Upon receiving notification, an investigation was launched to determine the scope and nature of any PrimeLending customer data that may have been impacted.

The review determined that the following personal information may be affected: name, account number, and routing number.

Notice to Maine Residents

On or about August 23, 2023, PrimeLending will begin providing written notice of this incident to potentially affected individuals, which includes approximately two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

While this incident did not occur at PrimeLending, it did occur at a vendor of PrimeLending's parent company, PlainsCapital. PrimeLending has been assured that as part of PlainsCapital's ongoing commitment to data security, PlainsCapital is reviewing its processes related to third-party vendors and data transfers. Further, PrimeLending's parent company notified federal law enforcement regarding the event.

PrimeLending is notifying potentially affected individuals and providing two (2) Maine residents with access to credit monitoring services for twelve (12) months at no cost. Additionally, PrimeLending is providing individuals with guidance on how to better protect against identity theft and fraud, including 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. PrimeLending is providing written notice of this incident to relevant state and federal regulators, as necessary.

EXHIBIT A

PrimeLending
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

August 23, 2023

Notice of Data Event

Dear [redacted]:

I'm writing to you from PrimeLending, a PlainsCapital Company ("PrimeLending"), to let you know about an event that may affect the security of your personal information. You are receiving this letter because your account information used to make payments to PrimeLending was impacted by the event. Below you'll find details about the event, our response, and the resources available to you to help protect your personal information from possible misuse. Please know that we greatly value the trust you place in us and this event is receiving the highest level of attention at our company.

What Happened. On or around July 24, 2023, we received notice from PrimeLending's parent company, PlainsCapital Bank ("PlainsCapital" or the "Bank"), that certain PrimeLending information was impacted by a global cyberattack conducted against MOVEit, a file transfer software used by one of the Bank's third-party vendors (the "Vendor") and by many government agencies, enterprise corporations, and leading technology and professional service organizations world-wide. A large number of these organizations globally have been impacted by this zero-day cyberattack. Neither PrimeLending nor PlainsCapital directly engages with MOVEit; however, Vendor, a leading financial technology service provider, utilizes the MOVEit software to deliver information associated with contracted information processing services, and was impacted by the incident (the "Vendor Incident"). Upon receiving notification, an investigation was immediately launched to determine the scope and nature of any PrimeLending customer data that may have been impacted. As a result of the Vendor Incident, we have determined that some of your information was likely obtained by an unauthorized party.

What Information Was Involved. While we are currently unaware of any identity theft or fraud occurring as result of this incident, the data that was likely impacted by the Vendor Incident includes your name, and the account number and routing number of the account you used to make payments to PrimeLending.

What Information Was NOT Involved. We do not have any indication your Social Security Number, online PrimeLending username or password were exposed. Please know that PrimeLending will NEVER call, text, or email you and ask for your username or password; do not share this information with anyone.

What We Are Doing. We at PrimeLending take this event and the security of the personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond to the event and notify potentially affected customers.. The Bank has also initiated a dialogue with the Vendor, and we have been assured that all software security patches have been applied to their affected systems.

As an added precaution, we are providing you with the option for complimentary access to 12 months of credit monitoring and identity restoration services provided by Cyberscout, a TransUnion company. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process yourself.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Your Personal Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against potential incidents of identity theft and fraud, to regularly review your account statements and transaction history, and to monitor your credit reports for suspicious activity over the next 12 to 24 months. You will also find information on how to enroll in the complimentary credit monitoring services offered.

For More Information. We greatly value your relationship with us here at PrimeLending, and protecting your personal information is a highest priority for us. I recognize that you may have questions not addressed in this letter. If so, we are here to help. Please don't hesitate to reach out in any of the following ways:

- Call 1-833-510-0372 to speak with an agent dedicated to answering questions about the incident.
- Call 1-800-597-0233 to speak with the PrimeLending servicing department.

I thank you for your ongoing business and for allowing us to serve your financial needs.

Sincerely,

Steve Thompson
President & CEO
PrimeLending, A PlainsCapital Company

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

In response to the incident, we are providing you with access to complimentary credit monitoring services for up to 12 months from your date of enrollment. These services provide you with same-day alerts when changes occur to your TransUnion credit file or updates take place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through IdentityForce, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/primelending** and follow the instructions provided. When prompted please provide the following unique code to receive services: **2QRCQCFDQN** Please note that the code is case-sensitive and must be entered exactly as it appears. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide the following information to each of the credit bureaus:

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. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a fraud alert or a credit freeze, 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	1-800-916-8800
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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 12224-0341; 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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.