

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

July 14, 2023

Notice of Data Event

,

I'm writing to you from PlainsCapital Bank (the "Bank") to let you know about an event that may affect the security of your personal information. You are receiving this letter because your personal account with us, or a business account that you are associated with, 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 as your financial institution, and this event is receiving the highest level of attention at our company.

What Happened. On June 27, 2023, one of the Bank's third-party vendors, a leading financial technology service provider (the "Vendor"), confirmed exposure to the global cyberattack conducted against MOVEit, a file transfer software deployed by many government agencies, enterprise corporations, and leading technology and professional service organizations world-wide (the "Vendor Incident"). A large number of these organizations globally have been impacted by this zero-day cyberattack. While MOVEit software is not directly contracted by the Bank, it is used by the Vendor to deliver information associated with contracted data processing services. Upon receiving notification from the Vendor, the Bank immediately launched an investigation to determine the scope and nature of any PlainsCapital Bank customer data that may have been impacted. As a result of the Vendor Incident, we 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

What Information Was NOT Involved. We do not have any indication that online and mobile banking usernames or passwords were exposed, nor were Personal Identification Numbers (PINs) used to perform debit card transactions. Please know that PlainsCapital Bank will NEVER call, text, or email you and ask for your username, password, or PIN; do not share this information with anyone.

What We Are Doing. We at PlainsCapital 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. We continue to vigilantly monitor for any signs of improper use, fraud, or access to customer accounts. We also initiated a dialogue with the Vendor, who has assured us 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 through Identity Force, 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 PlainsCapital, 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 your account officer
- Call your local branch
- Call 1-888-976-2552 to speak with an agent dedicated to answering questions about the incident
- Call 1-866-762-8392 to speak with the PlainsCapital Customer Service team

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

Sincerely,

Jerry Schaffner
President & CEO
PlainsCapital Bank

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 twenty-four (24) months from your date of enrollment. These services provide you with same-day alerts when changes occur to your 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/plainscapital** and follow the instructions provided. When prompted please provide the following unique code to receive services: 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.

0000102028000

P

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.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/.

For 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 bureaus 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 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. We encourage you to 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.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 10 Rhode Island residents impacted by this event.