



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

January 11, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to the Maryland resident was contained in the potentially impacted data: name and Social Security number. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Maryland Resident

On or about January 11, 2024, Bi-State began providing written notice of this incident to one (1) Maryland resident. 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

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT A



January 11, 2024

NOTICE OF DATA BREACH

Dear:

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to further protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to you was contained in the potentially impacted data: name, Social Security number, bank account information, and health insurance. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Further Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Further Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

0000102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. – 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev> and follow the instructions provided. When prompted please provide the following unique code to receive services: ;;;;;;;;;;. 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 years of age. 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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

March 1, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to supplement our January 11, 2024, notice to your office. This previous notice is attached hereto as ***Exhibit AA***. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of the data potentially at risk and on February 7, 2024, the investigation determined that the following information related to Maryland residents was contained in the potentially impacted data: name, and Social Security number. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Maryland Residents

On or about January 11, 2024, Bi-State began providing written notice of this incident to three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Bi-State 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT AA

From: Alexis Childs
Sent: Thursday, January 11, 2024 4:30 PM
To: databreach@ilag.gov
Cc: Gregory Bautista; Hannah Lukatchik
Subject: Bi-State Development - Notice of Data Event - IL
Attachments: Bi-State Development - Notice of Data Event - IL.pdf

Categories: zM:Bi-State Development - Oct 2023 - RW - Claim No. NGP-23-02508--576-085

To Whom It May Concern,

Please see the attached notice of data event.

Thank you,
Alexis

Alexis Childs
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-1361 - Office
(551) 655-8154 - Mobile
achilds@mullen.law



This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

January 11, 2024

VIA E-MAIL

Office of the Illinois Attorney General
100 West Randolph Street
Chicago, IL 60601
E-mail: databreach@ilag.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one thousand eight hundred six (1806) Illinois residents. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Illinois law, the applicability of the Illinois data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to Illinois residents was contained in the potentially impacted data: name, Social Security number, driver’s license, passport number, bank account information, health insurance, and medical information. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Illinois Residents

On or about January 11, 2024, Bi-State began providing written notice of this incident to one thousand eight hundred six (1806) Illinois 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

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT A

Bi-State Development Agency of the Missouri-Illinois
Metropolitan District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



January 11, 2024

NOTICE OF DATA BREACH

Dear:

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to further protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to you was contained in the potentially impacted data: name, Social Security number, bank account information, and health insurance. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Further Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Further Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

0000102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. – 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev> and follow the instructions provided. When prompted please provide the following unique code to receive services: ;;;;;;;;;;. 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 years of age. 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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.

EXHIBIT B



March 1, 2024

NOTICE OF SECURITY INCIDENT

Dear:

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to you was contained in the potentially impacted data: name, Social Security number. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

0000102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. – 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev> and follow the instructions provided. When prompted please provide the following unique code to receive services: XXXXXXXX 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 years of age. 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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 <https://ncdoj.gov/>.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

April 18, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to supplement our March 1, 2024, notice to your office. This previous notice is attached hereto as ***Exhibit C***. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of its internal systems to review the data potentially at risk and obtain available address information related to the potentially impacted individuals. The investigation determined that the following information related to Maryland residents was contained in the potentially impacted: name, Social Security number and medical information. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Maryland Residents

On or about January 11, 2024, Bi-State began notifying impacted Maryland residents. This notice is to inform your Office that Bi-State is providing written notice of this incident to an additional fifteen (15) Maryland residents. For context, the review of data potentially at-risk continued and affected individuals were notified on a rolling basis. On March 25, 2024, additional individuals were identified as potentially impacted and available address information related to the potentially impacted individuals was obtained. On April 18, 2024, Bi-State provided written notice of this incident to the additional individuals determined to be potentially impacted, including fifteen (15) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit D***.

Other Steps Taken and To Be Taken

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Bi-State 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT C

From: Alexis Childs
Sent: Friday, March 1, 2024 7:36 PM
To: idtheft@oag.state.md.us
Cc: Gregory Bautista; Hannah Lukatchik; Alexis Childs
Subject: Bi-State Development - Supplemental Notice of Data Event - MD
Attachments: Bi-State Development - Supplemental Notice of Data Event - MD.pdf

Categories: zM:Bi-State Development - Oct 2023 - RW - Claim No. NGP-23-02508--576-085

To Whom It May Concern:

Please find attached the supplemental notice of data event.

Thank you,
Alexis & Greg

Alexis Childs
Attorney
Mullen Coughlin LLC
75 S Clinton Ave Suite 510
Rochester, NY 14604
(267) 930-1361 - Office
(551) 655-8154 - Mobile
achilds@mullen.law

This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

March 1, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to supplement our January 11, 2024, notice to your office. This previous notice is attached hereto as ***Exhibit AA***. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of the data potentially at risk and on February 7, 2024, the investigation determined that the following information related to Maryland residents was contained in the potentially impacted data: name, and Social Security number. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Maryland Residents

On or about January 11, 2024, Bi-State began providing written notice of this incident to three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Bi-State 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT AA

From: Alexis Childs
Sent: Thursday, January 11, 2024 4:30 PM
To: databreach@ilag.gov
Cc: Gregory Bautista; Hannah Lukatchik
Subject: Bi-State Development - Notice of Data Event - IL
Attachments: Bi-State Development - Notice of Data Event - IL.pdf

Categories: zM:Bi-State Development - Oct 2023 - RW - Claim No. NGP-23-02508--576-085

To Whom It May Concern,

Please see the attached notice of data event.

Thank you,
Alexis

Alexis Childs
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-1361 - Office
(551) 655-8154 - Mobile
achilds@mullen.law



This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

January 11, 2024

VIA E-MAIL

Office of the Illinois Attorney General
100 West Randolph Street
Chicago, IL 60601
E-mail: databreach@ilag.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Bi-State Development (“Bi-State”) located at 211 North Broadway, Suite 700, St. Louis, MO 63102-2759, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one thousand eight hundred six (1806) Illinois residents. By providing this notice, Bi-State does not waive any rights or defenses regarding the applicability of Illinois law, the applicability of the Illinois data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 2, 2023, Bi-State discovered suspicious activity on its network. Bi-State immediately took systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, Bi-State investigated this incident to determine whether any sensitive information was viewed or removed from Bi-State’s systems without authorization. The investigation determined that an unknown actor gained access to certain parts of their network on October 1, 2023.

Following this determination, Bi-State worked as quickly as possible to review the documents to determine those individuals whose information was present and notify them about this incident. Bi-State undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to Illinois residents was contained in the potentially impacted data: name, Social Security number, driver’s license, passport number, bank account information, health insurance, and medical information. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Illinois Residents

On or about January 11, 2024, Bi-State began providing written notice of this incident to one thousand eight hundred six (1806) Illinois 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

Upon discovering the event, Bi-State moved quickly to investigate and respond to the incident, assess the security of Bi-State systems, and identify potentially affected individuals. Further, Bi-State notified federal law enforcement regarding the event. Bi-State is also working to implement additional safeguards. Bi-State is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bi-State is providing impacted 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.

Bi-State is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Bi-State is unaware whether law enforcement is currently investigating the event in response to Bi-State's notification regarding the event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT A

Bi-State Development Agency of the Missouri-Illinois
Metropolitan District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



January 11, 2024

NOTICE OF DATA BREACH

Dear:

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to further protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to you was contained in the potentially impacted data: name, Social Security number, bank account information, and health insurance. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Further Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Further Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

0000102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. – 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev> and follow the instructions provided. When prompted please provide the following unique code to receive services: **XXXXXXXXXX**. 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 years of age. 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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.

EXHIBIT B

Bi-State Development Agency of the Missouri-Illinois
Metropolitan District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



March 1, 2024

NOTICE OF SECURITY INCIDENT

Dear:

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on November 30, 2023, the investigation determined that the following information related to you was contained in the potentially impacted data: name, Social Security number. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

0000102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. – 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev> and follow the instructions provided. When prompted please provide the following unique code to receive services:

XXXXXXX 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 years of age. 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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 <https://ncdoj.gov/>.

EXHIBIT D

Bi-State Development Agency of the Missouri-Illinois
Metropolitan District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



April 18, 2024

NOTICE OF SECURITY INCIDENT

Dear :

Bi-State Development is writing to inform you of a recent event which may impact some of your personal information. While there is no evidence of actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about this event, our response, and the steps you may take, if you haven't already done so, to further protect your information against identity theft and fraud.

What Happened? On October 2, 2023, Bi-State Development discovered suspicious activity on our network. We moved quickly to secure the systems and launched an investigation to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems. As a result, the unknown actor may have had access to certain files within these systems and information may have been accessed or acquired.

What Information Was Involved? As part of the investigation, we undertook a time intensive review of the data potentially at risk and on March 25, 2024, the investigation determined that the following information related to you was contained in the potentially impacted data: your name, and Social Security number. We have no evidence this information has been subject to actual or attempted misuse.

What Is Bi-State Development Doing? The privacy and security of your information is among our highest priorities. Upon discovering the event, we moved quickly to respond and investigate the event, assess the security of our systems, and notify potentially impacted individuals. Additionally, we have been in communication with federal law enforcement regarding this event and are assisting in their investigation. We are also notifying appropriate regulators and consumer reporting agencies, as required.

As an added precaution, we are providing all team members twelve (12) months of free credit monitoring through TransUnion. Enrollment instructions can be found in the attached *Steps You Can Take to Further Protect Your Personal Information*. Please note, you must enroll in credit monitoring yourself as Bi-State Development is unable to do so on your behalf.

What Can You Do? Enroll in the free credit monitoring service. 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 *Steps You Can Take to Further Protect Your Personal Information*, including additional information on what you can do to better protect your information against misuse, should you feel it necessary to do so.

000010102G0500

P

Need More Information? We understand you may have questions about this event that are not addressed in this letter. Please call the dedicated TransUnion Call Center number at 1-833-540-0844 Monday through Friday from 7 a.m. - 7 p.m. Central time, excluding holidays, for additional assistance.

You can also send written questions to Bi-State Development at 211 N. Broadway, Attn: Risk Management, Suite 700, St. Louis, Missouri 63102.

Sincerely,
Bi-State Development

Steps You Can Take to Further Protect Your Personal Information

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, 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/bistatedev>** and follow the instructions provided. When prompted please provide the following unique code to receive services: XXXXXXXXXX. 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 years of age. 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.

00001020280000

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 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.