Mullen Coughlin LLC
Attorneys at Law

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

January 3, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Albright Capital Management LP ("Albright"), located at 1101 Wilson Blvd., Fl. 6, Arlington, VA 22209-2281, and are writing to notify your office of an event that may affect the security of some personal information relating to twelve (12) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Albright 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 or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and took information contained in those systems.

Albright reviewed the information accessible within the systems to identify individuals with information potentially at risk. On November 19, 2021, Albright finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. The personal information impacted by this event includes the following: name, address, date of birth, Social Security number, other state or federal identification number, passport number, driver's license, financial account information, health insurance information, and electronic/digital signature.

Notice to Maryland Residents

On or about January 3, 2022, Albright provided written notice of this event to all affected individuals, which includes twelve (12) Maryland 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, Albright moved quickly to investigate and respond to the event, assess the security of Albright systems, and notify potentially affected individuals. Albright is also working to implement additional safeguards and training to its employees. Albright is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Albright is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Albright 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/eks
Enclosure

Exhibit A

Albright Capital

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<DATA BREACH>>

Dear <<Name 1>>:

Albright Capital Management LP ("Albright") is writing to inform you of a recent event that may impact the security of some of your information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and that information contained in those systems was taken by the unauthorized actor. Therefore, we conducted a review of the information accessed and accessible within the systems to identify individuals with personal information that could have been accessible during the event. We concluded this review on November 19, 2021. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, <<Variable Text 1>> were accessed or accessible within the systems at the time of this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, and although we do not have any indication of any actual or attempted misuse of your personal information, we are offering credit monitoring and identity theft protection services through TransUnion for <<Variable Text 2>> months at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-604-1709, Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, excluding major U.S. holidays. Please have your activation code ready. Again, we take the privacy and security of personal information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Gregory Bowes
Managing Principal
Albright Capital Management LP
www.albrightcapital.com

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Variable Text 2>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<< Insert static 6-digit Telephone Pass Code >>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<Variable Text 2>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Insert Date>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place 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	1-833-395-6938
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; 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 www.oag.state.md.us. Albright Capital Management is located at 601 13th St., NW #1000, Washington, DC 20005.

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/.

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

February 15, 2022

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

Dear Sir or Madam:

We represent Albright Capital Management LP ("Albright"), located at 1101 Wilson Blvd., Fl. 6, Arlington, VA 22209-2281, and are writing to notify your office of an event that may affect the security of some personal information relating to twenty (20) Maryland residents. This notice supplements the initial notice submitted to your Office on behalf of Albright on January 3, 2022. This notice will be further supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Albright 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 or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and took information contained in those systems.

Albright reviewed the information accessible within the systems to identify individuals with information potentially at risk. On November 19, 2021, Albright finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. The personal information impacted by this event includes the following: name, address, date of birth, Social

Security number, other state or federal identification number, passport number, driver's license, financial account information, health insurance information, and electronic/digital signature.

Notice to Maryland Residents

On or about January 3, 2022, Albright began providing written notice of this event to affected individuals, including twelve (12) Maryland residents. On or about February 15, 2022, Albright also mailed notice to an additional eight (8) Maryland residents. Written notice was and is being provided in substantially the same form as the letters attached here as ***Exhibit A***. A copy of the initial notice submitted to your Office on behalf of Albright is also attached here as ***Exhibit B.***

Other Steps Taken and To Be Taken

Upon discovering the event, Albright moved quickly to investigate and respond to the event, assess the security of Albright systems, and notify potentially affected individuals. Albright is also working to implement additional safeguards and training to its employees. Albright is providing access to credit monitoring services for one (1) year, through either TransUnion or Equifax, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Albright is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Albright 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/eks
Attachments

EXHIBIT A
TO THE
SUPPLEMENTAL
NOTICE

Albright Capital

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>>:

Albright Capital Management LP ("Albright") is writing to inform you of a recent event that may impact the security of some of your information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and that information contained in those systems was taken by the unauthorized actor. Therefore, we conducted a review of the information accessed and accessible within the systems to identify individuals with personal information that could have been accessible during the event. We concluded this review on November 19, 2021. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, <<Variable Text 1>> were accessed or accessible within the systems at the time of this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, and although we do not have any indication of any actual or attempted misuse of your personal information, we are offering credit monitoring through Equifax for 12 months at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-604-1709, Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, excluding major U.S. holidays. Please have your activation code ready. Again, we take the privacy and security of personal information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Gregory Bowes
Managing Principal
Albright Capital Management LP
www.albrightcapital.com

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Enter your Activation Code: ***<ACTIVATION CODE>***
Enrollment Deadline: ***<DEADLINE MMMM DD, YYYY>***

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<ACTIVATION CODE>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place 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	1-833-395-6938
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; 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 www.oag.state.md.us. Albright Capital Management is located at 601 13th St., NW #1000, Washington, DC 20005.

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/.

Albright Capital

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
Parent or Guardian of
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF SECURITY INCIDENT

Dear Parent or Guardian of <<Name 1>>:

Albright Capital Management LP ("Albright") is writing to inform you of a recent event that may impact the security of some of your minor child's information. Although we have received no indication of any actual or attempted misuse of your minor child's information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your minor child's information from possible misuse, should you feel it is necessary to do so.

What Happened? On or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and that information contained in those systems was taken by the unauthorized actor. Therefore, we conducted a review of the information accessed and accessible within the systems to identify individuals with personal information that could have been accessible during the event. We concluded this review on November 19, 2021. Although we are unaware of any actual or attempted misuse of your minor child's personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your minor child's name, address, <<Variable Text 1>> were accessed or accessible within the systems at the time of this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you on your minor child's behalf, so that you may take further steps to best protect your minor child's information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, and although we do not have any indication of any actual or attempted misuse of your minor child's personal information, we are offering identity monitoring and theft protection services through Equifax for <<Variable Text 2>> months at no cost to you or your minor child.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing for any suspicious activities related to the use of your minor child's information, including with respect to any financial or other accounts in your minor child's name. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Your Minor Child's Personal Information*. You may also enroll in the complimentary identity monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-604-1709, Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, excluding major U.S. holidays. Please have your activation code ready. Again, we take the privacy and security of personal information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you and your minor child.

Sincerely,

Gregory Bowes
Managing Principal
Albright Capital Management LP
www.albrightcapital.com

Steps You Can Take to Protect Your Minor Child's Personal Information

<u>Enroll in Credit Monitoring – Equifax Child Monitoring Package</u>

Activation Code: ***<<ACTIVATION CODE>>***
Enrollment Deadline: ***<<DEADLINE MMMM DD, YYYY>>***

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications to the primary adult member of activity on the child's Equifax credit report

Enrollment Instructions
Parent/guardian Go to ***www.equifax.com/activate***
Enter your unique Activation Code of ***<ACTIVATION CODE>*** then click "Submit" and follow these 4 steps:

1. **<u>Register</u>:** Complete the form with parent/guardian contact information and click "Continue". *If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.*
2. **<u>Create Account</u>:** Enter parent/guardian email address, create a password, and to accept the terms of use.
3. **<u>Verify Identity</u>:** To enroll in your product, we will ask you to complete our identity verification process.
4. **<u>Checkout</u>:** Upon successful verification of parent/guardian identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows parent/guardian completed enrollment. Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package
You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child"
3. From there, enter your child's first name, last name, date of birth and social security number.

Repeat steps for each minor child (up to four)

Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.

<u>Monitor Your Accounts</u>

Although minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established:

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.

Adults 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 security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or 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	1-833-395-6938
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; 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 www.oag.state.md.us. Albright Capital Management is located at 601 13th St., NW #1000, Washington, DC 20005.

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/.

EXHIBIT B
TO THE
SUPPLEMENTAL
NOTICE

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

January 3, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Albright Capital Management LP ("Albright"), located at 1101 Wilson Blvd., Fl. 6, Arlington, VA 22209-2281, and are writing to notify your office of an event that may affect the security of some personal information relating to twelve (12) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Albright 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 or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and took information contained in those systems.

Albright reviewed the information accessible within the systems to identify individuals with information potentially at risk. On November 19, 2021, Albright finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. The personal information impacted by this event includes the following: name, address, date of birth, Social Security number, other state or federal identification number, passport number, driver's license, financial account information, health insurance information, and electronic/digital signature.

Notice to Maryland Residents

On or about January 3, 2022, Albright provided written notice of this event to all affected individuals, which includes twelve (12) Maryland 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, Albright moved quickly to investigate and respond to the event, assess the security of Albright systems, and notify potentially affected individuals. Albright is also working to implement additional safeguards and training to its employees. Albright is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Albright is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Albright 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Riesgo Jensen

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/eks
Enclosure

Exhibit A

Albright
Capital

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<DATA BREACH>>

Dear <<Name 1>>:

Albright Capital Management LP ("Albright") is writing to inform you of a recent event that may impact the security of some of your information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On or about September 26, 2021, Albright discovered suspicious activity on its network. Albright immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before that date, an unauthorized actor gained access to certain Albright systems and that information contained in those systems was taken by the unauthorized actor. Therefore, we conducted a review of the information accessed and accessible within the systems to identify individuals with personal information that could have been accessible during the event. We concluded this review on November 19, 2021. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, <<Variable Text 1>> were accessed or accessible within the systems at the time of this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, and although we do not have any indication of any actual or attempted misuse of your personal information, we are offering credit monitoring and identity theft protection services through TransUnion for <<Variable Text 2>> months at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-604-1709, Monday through Friday, between 9:00 AM and 9:00 PM Eastern time, excluding major U.S. holidays. Please have your activation code ready. Again, we take the privacy and security of personal information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Gregory Bowes
Managing Principal
Albright Capital Management LP
www.albrightcapital.com

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Variable Text 2>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<< Insert static 6-digit Telephone Pass Code >>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<Variable Text 2>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Insert Date>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place 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	1-833-395-6938
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; 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 www.oag.state.md.us. Albright Capital Management is located at 601 13th St., NW #1000, Washington, DC 20005.

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/.