

RECEIVED

SEP 28 2021



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

CONSUMER PROTECTION

Kevin M. Mekler  
Office: (267) 930-2190  
Fax: (267) 930-4771  
Email: [Kmekler@mullen.law](mailto:Kmekler@mullen.law)

3001 N Rocky Point Drive East, Suite 200  
Tampa, FL 33607

September 24, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Madame or Sir:

We represent Main Line Investment Partners and its affiliated/related entities: MainLine Securities LLC, Merion Realty Partners, Merion Residential, and MainLine Private Wealth (“MainLine”) located at 308 E Lancaster Avenue, Suite 300, Wynnewood, PA 19096, and are writing to notify your office of an incident that may affect the security of some personal information relating to thirty nine (39) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MainLine does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about July 20, 2021, MainLine discovered that certain files on its network were encrypted with malware by an unknown actor. MainLine promptly took steps to secure its network and launched an investigation to determine the nature and scope of the event. While the investigation into the full scope of the event is ongoing, the investigation did determine that certain files may have been accessed or acquired by the unknown actor. MainLine then promptly undertook a thorough and time intensive review of these files to determine the individuals whose information was at risk or acquired, and then worked to quickly identify accurate address information to notify these individuals of the event.

The information that could have been subject to unauthorized access includes name, address, social security number, government issued identification, and/or financial account information.

[Mullen.law](http://Mullen.law)

### **Notice to New Hampshire Residents**

On or about September 24, 2021, MainLine provided written notice of this incident to all affected individuals, which includes thirty nine (39) New Hampshire 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, MainLine moved quickly to investigate and respond to the incident, assess the security of MainLine systems, and notify potentially affected individuals. MainLine is also working with cyber security specialists, implementing additional safeguards, and providing additional training to its employees to reduce the likelihood of similar events occurring in the future. MainLine is also providing access to credit monitoring services for one (1) year through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MainLine 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. MainLine is providing individuals with information on how to place a fraud alert and credit freeze on one's credit file, information on protecting against tax fraud, 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 security event, please contact us at (267) 930-2190.

Very truly yours,



Kevin M. Mekler of  
MULLEN COUGHLIN LLC

KMK/jxg  
Enclosure

# **EXHIBIT A**



MainLine Investment Partners  
10300 SW Greenburg Rd. Suite 570  
Portland, OR 97223

To Enroll, Please Call:  
1-800-939-4170  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

September 24, 2021

Dear <<First Name>> <<Last Name>>,

MainLine Investment Partners, and/ one or more of its affiliated/related entities: MainLine Private Wealth, Merion Realty Partners, CMS Companies, and Merion Residential (“MainLine”), writes to inform you of an event that may impact some of your information. While there is no evidence of attempted or actual misuse of your information, we are providing you with information about this event, our response, and the steps you may take to further protect your information against identity theft and fraud, should you feel it necessary to do so.

**What Happened?**

On July 20, 2021, MainLine became aware that certain files on its computer system were encrypted with malware by an unknown actor. MainLine promptly took steps to secure the impacted systems and its network and launched an investigation to determine the nature and scope of the event. While the investigation into the full scope of the incident is ongoing, the investigation determined that certain files may have been accessed by an unauthorized individual. MainLine then promptly undertook a thorough and time intensive review of the data to determine the individuals whose information was at risk, and then worked quickly to identify accurate address information to provide this written notification to all potentially impacted individuals.

**What Information Was Involved?**

While the investigation has been able to determine which systems were accessed, we have not been able to determine definitively if your data was accessed or acquired. However, we are providing you this notice out of an abundance of caution as your information may be at risk. This information includes your name, address, social security number, government issued identification, and/or financial account information.

**What We Are Doing.**

The privacy and security of your information is among our highest priorities and we take this incident very seriously. MainLine is reviewing its security policies and procedures, as well as working with a cybersecurity specialist, to reduce the risk of this happening in the future. MainLine is also implementing additional measures and security tools to further protect the information on our systems, and also working to provide employees with additional training regarding data privacy and security. While we do not have any indication of fraud or identity theft occurring as a result of this incident, we are offering <<12/24>> free months of credit monitoring through IDX as an added precaution. We have also reported this incident to federal law enforcement and are notifying all relevant regulators, as required.

**What You Can Do.**

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Additional information and resources are included in the enclosed *Steps You Can Take To Help Protect Your Information*. You may also enroll in the complimentary credit monitoring available to you at no cost. Enrollment instructions are also attached to this letter.

**For More Information.**

If you have any additional questions, please call our dedicated assistance line at 1-800-939-4170 Monday through Friday from 9 am - 9 pm Eastern Time. You may also write to c/o MainLine at 308 E. Lancaster Avenue, Suite 300, Wynnewood, PA 19096 or reach out to investor services or your primary contact in our organization.

Sincerely,

*MainLine*

## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Enroll in Credit Monitoring**

**1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

IDX identity protection services includes credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note the deadline to enroll is December 31, 2021.

**3. Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze you 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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	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](http://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](mailto: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](http://www.oag.state.md.us). MainLine is located at 308 E. Lancaster Avenue, Suite 300, Wynnewood, PA 19096.

*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](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 5 Rhode Island residents impacted by this incident.