



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

RECEIVED

OCT 20 2020

CONSUMER PROTECTION

Edward J. Finn  
Office: (267) 930-4776  
Fax: (267) 930-4771  
Email: [efinn@mullen.law](mailto:efinn@mullen.law)

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

October 9, 2020

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

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Readerlink Distribution Services, LLC (“Readerlink”) located at 1420 Kensington Road, Suite 300, Oak Brook, IL 60523, and are writing to notify your office of an incident that may affect the security of personal information relating to approximately fourteen (14) New Hampshire residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Readerlink does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

#### **Nature of the Data Event**

On June 13, 2020, Readerlink learned that it was the victim of a malware attack that encrypted certain systems. Readerlink worked quickly to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption and (3) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, information by the unknown actor.

Readerlink conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. The investigation identified that certain Readerlink systems were accessed by an unknown actor between June 3, 2020 and June 13, 2020, and certain data was exfiltrated from Readerlink’s systems. Some of this data was posted by the bad actor on or around June 17, 2020. Readerlink then worked to determine the identities and contact information for potentially impacted individuals. On or about June 24, 2020 Readerlink confirmed the identities of the individuals who did or who may have had information posted on June 17, 2020 and provided notice and credit monitoring and identity restoration services to them. On August 15, 2020, the bad actor posted additional information. Readerlink again

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

worked to determine the identities and contact information for individuals in the additional files posted. Readerlink recently confirmed contact information for these individuals and began providing notification and offering credit monitoring and identity restoration services to them, as well.

Although the types of personal information potentially impacted varies by individual, the types of personal information affected for New Hampshire residents includes: names, addresses, Social Security numbers, and W-2 wage and tax information.

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

On June 16, June 18, and June 19, 2020, Readerlink provided initial notice of this event via email and letter to potentially affected employees as the investigation was ongoing. From June 26, 2020 to July 10, 2020, Readerlink provided written notice of this incident to individuals who were affected or who may have been affected by the June 17, 2020 posting. On October 7, 2020, Readerlink provided written notice to the individuals whose information was posted on August 15, 2020, which includes approximately fourteen (14) New Hampshire residents. Written notice was provided to affected individuals in substantially the same form as the letters attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the ransomware event, Readerlink moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. Readerlink is also working to implement additional safeguards to protect the security of information in its systems. Readerlink has notified federal law enforcement.

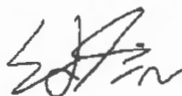
Readerlink is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to credit monitoring and identity restoration services through Kroll, and the contact information for a dedicated assistance line for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Readerlink is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Readerlink also provided written notice of this incident to other regulators, as necessary.

Consumer Protection Bureau  
October 9, 2020  
Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

A handwritten signature in black ink, appearing to read "E. Finn".

Edward Finn of  
MULLEN COUGHLIN LLC

EJF:zlg  
Enclosure

# **EXHIBIT A**



READERLINK®

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Readerlink Distribution Services, LLC ("Readerlink") is writing to inform you of a recent event that may impact the security of some of your information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On June 13, 2020, Readerlink learned that it was the victim of a malware attack that encrypted certain systems. Readerlink worked quickly to: (1) secure the systems; (2) restore access to the information so it could continue to operate the business without disruption and (3) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, information by the unknown actor.

Readerlink conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. Although our investigation is ongoing, current evidence shows that certain Readerlink systems were accessed by an unknown actor between approximately June 3, 2020 and June 13, 2020, and certain data was copied and taken from our systems. Some of this data was posted online by the bad actor on or around June 17, 2020. At that time, your personal data was not posted. However, the bad actor later, on or about August 15, 2020, posted additional information. We again worked to determine the identities and contact information for potentially impacted individuals in the additional files posted.

**What Information Was Involved.** We have determined the following types of information were present in Readerlink's system and that the potentially affected information acquired by the unknown actor during this incident differs for each individual and may include the following relating to you: name, address, Social Security number, and W-2 wage and tax information.

**What We Are Doing.** We take this incident and the security of your personal information very seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our existing policies and procedures and implementing additional safeguards to further secure the information in our systems, including personal information. Readerlink also notified federal law enforcement and other government regulators. Although your personal information was not posted in June, we previously offered you access to 12 months of credit monitoring and identity restoration services through Kroll. We are providing you another code and activation instructions to use and encourage you to activate the code now.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank and credit card account statements, and to monitor your credit reports for suspicious activity. You may also activate the complimentary identity monitoring services described above. Enrollment instructions were previously provided to you, and enrollment information can be provided, if you no longer have it.

**For More Information.** If you have additional questions, please email us at [info-questions@readerlink.com](mailto:info-questions@readerlink.com) or call our dedicated assistance line at 708-234-4003, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time (excluding U.S. holidays). You may also write to Readerlink at 1420 Kensington Road, Suite 300, Oak Brook, IL 60523.

We understand and sincerely regret the inconvenience and concern this incident may cause.

Sincerely,

Readerlink Distribution Services, LLC



## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Activation Instructions**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **December 30, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To sign in to your account after you have activated your identity monitoring services, please visit <https://login.idheadquarters.com/>

### **Identity Monitoring Services**

You've been provided with access to the following services<sup>1</sup> from Kroll:

#### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can 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 New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



READERLINK®

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Readerlink Distribution Services, LLC ("Readerlink") is writing to inform you of a recent event that may impact the security of some of your information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On June 13, 2020, Readerlink learned that it was the victim of a malware attack that encrypted certain systems. Readerlink worked quickly to: (1) secure the systems; (2) restore access to the information so it could continue to operate without disruption; and (3) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, information by the unknown actor.

Readerlink conducted an extensive investigation, with the assistance of third-party computer forensic specialists, to determine the nature and scope of the incident. Although our investigation is ongoing, current evidence shows that certain Readerlink systems were accessed by an unknown actor between June 3, 2020 and June 13, 2020, and certain data was exfiltrated from our systems. Some of this data was posted online by the bad actor on or around June 17, 2020. At that time, your personal data was not posted. However, the bad actor later, on or about August 15, 2020, posted additional information. We, again, worked to determine the identities and contact information for potentially impacted individuals in the additional files posted.

**What Information Was Involved.** We have determined the following types of information were in the impacted systems and potentially acquired by the attacker and may include the following relating to you: name, address, Social Security number, and W-2 wage and tax information.

**What We Are Doing.** We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to further secure our systems and restore our operations. As part of our ongoing commitment to the privacy of personal information in our possession, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Readerlink also notified federal law enforcement and other government regulators. In an abundance of caution, we are offering you access to 12 months of identity monitoring services through Kroll, which will be paid for by Readerlink. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

**What You Can Do.** You can find out more about how to help protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank and credit card account statements, and to monitor your credit reports for suspicious activity. You may also activate the complimentary identity monitoring services described above. Activation instructions are attached to this letter.

**For More Information.** If you have additional questions, please call our dedicated assistance line at 1-844-951-2884, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time (excluding U.S. holidays). You may also write to Readerlink at 1420 Kensington Road, Suite 300, Oak Brook, IL 60523.

We understand and sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Readerlink Distribution Services, LLC



## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### **Activation Instructions**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **December 30, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

### **Identity Monitoring Services**

You've been provided with access to the following services<sup>1</sup> from Kroll:

#### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

### **Monitor Your Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. 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 contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

PO Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 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 agencies listed below:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can 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 Maryland residents:** The Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202 1-410-528-8662; and [www.oag.state.md.us](http://www.oag.state.md.us).

**For North Carolina residents:** The 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). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For New Mexico residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 Rhode Island residents:** The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 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 10 Rhode Island residents impacted by this incident.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>.

**For Washington, D.C. residents:** The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and [www.oag@dc.gov](mailto:www.oag@dc.gov).