



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

RECEIVED

DEC 16 2019

Ryan C. Loughlin  
Office: 267-930-4786  
Fax: 267-930-4771  
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

December 10, 2019

**INTENDED FOR ADDRESSEE(S) ONLY**

**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 Sir or Madam:

We represent Disability Insurance Specialists LLC (“DIS”) headquartered at 1280 Blue Hills Ave, Suite 102, Bloomfield, Connecticut 06002 and are writing on behalf of DIS and its impacted business partners to notify your office of an incident that may affect the security of personal information relating to certain individuals affiliated with DIS’ business partners. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, DIS 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 July 9, 2019, DIS became aware of unusual activity in an employee’s email account related to a phishing email campaign. DIS launched an investigation to determine what happened and what information may have been affected. The affected employee’s email account password was changed. With the assistance of computer forensics experts, DIS determined that a single email account was accessed without authorization on July 9, 2019.

DIS undertook a lengthy review of the email accounts to determine if any information was subject to unauthorized access. When the investigation could not rule out the possibility of such access, DIS engaged in a programmatic and manual review of the email account to determine if personal information existed in the account at the time of the incident. Following the conclusion of that review, on September 25, 2019, DIS confirmed that certain personal information may have been accessible to the unauthorized actor, and took steps to confirm address information for the potentially impacted individuals for purposes of providing notification to those individuals. These steps included further manual review to identify the entity that

provided the information to DIS and working with these entities to locate address information for those individuals to be notified. This process is ongoing.

Through this review DIS determined that the following types of information were accessible within the account: name and Social Security number.

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

On or about December 10, 2019, DIS continued providing written notice of this incident to affected individuals whose personal information may have been accessible within the account, which includes two (2) 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**

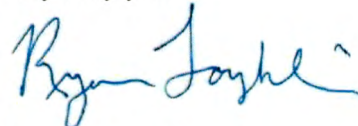
Upon discovering the event, DIS moved quickly to investigate and respond to the incident, assess the security of DIS's systems, and notify potentially affected individuals. DIS is providing individuals with information accessible within the account access to two (2) years of complimentary credit monitoring services.

Additionally, DIS 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. DIS 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. DIS is notifying state regulators and the consumer reporting agencies as necessary.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of  
MULLEN COUGHLIN LLC

RCL: ajd  
Enclosure

# EXHIBIT A



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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Disability Insurance Specialists, LLC, ("DIS") administers insurance claims for various insurers, including Lincoln National, the reinsurer for your New York Life disability policy administered by the Paul Revere Life Insurance Company. We are writing to notify you of a recent incident that may affect the security of some of your personal information received by DIS in the course of providing services related to your policy. While there is currently no evidence that your information has been misused, we are providing you with information regarding the event, measures we have taken, and what you may do to better protect your personal information should you feel it appropriate to do so. This incident will not affect any current or future claims for benefits you may have under your policy.

**What Happened?** On July 9, 2019, DIS became aware of suspicious activity related to a DIS employee's email account. Following the discovery of the suspicious activity, DIS launched an investigation to determine the full nature and scope of the activity. As part of our internal investigation, we reviewed a sampling of email contents and determined on July 19, 2019, that the account may contain personal information. With the assistance of leading computer forensics experts, we learned on August 30, 2019, that the DIS employee's email account was accessed without authorization on July 9, 2019. Unfortunately, the investigation was not able to determine which emails, if any, were actually accessed or viewed.

Working with these third-party experts, DIS undertook a comprehensive review of the impacted email account to confirm its earlier findings on the contents of the email account and identify those who may have personal information accessible within the impacted account. Although, to date, we are unaware of any actual or attempted misuse of your personal information, we are notifying you in an abundance of caution because your information was present in the impacted email account at the time of the incident.

**What Information Was Involved?** Our investigation confirmed the information present within the impacted email account at the time of the incident includes your <<ClientDef1(Impacted Data)>>.

**What Are We Doing?** Information privacy and security are among our highest priorities. DIS has strict measures in place to protect information in our care. Upon learning of this incident, DIS took steps to confirm and further strengthen the security of our systems, including our email accounts. As a precautionary measure, DIS continues to review its security policies and procedures as part of its ongoing commitment to information security.

While to date, we have no evidence of actual or attempted misuse of your personal information, we secured the services of Kroll to provide identity monitoring services at no cost to you for two (2) years. Information on how to activate this service may be found in the enclosed "Steps You Can Take to Help Protect Against Identity Theft and Fraud."

**What You Can Do.** 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. You may review the information contained in the enclosed "Steps You Can Take to Help Protect Against Identity Theft and Fraud" for guidance on how to better protect your personal information. You may also activate the identity monitoring services we are making available to you as we are unable to activate these services on your behalf.

***For More Information.*** We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-833-943-1374 which can be reached Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

DIS takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

John E. Sahlman  
VP Administration  
Disability Insurance Specialists, LLC

## Steps You Can Take to Help Protect Against Identity Theft and Fraud

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 two (2) years. 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<sup>1</sup> include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

### How to Activate Your Identity Monitoring Services

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

You have until **March 6, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

You've been provided with access to the following services 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.

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  
Chester, PA 19016  
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)

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;

<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.

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:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a>	<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	--

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); 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 North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [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 Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.oag.state.md.us](http://www.oag.state.md.us).

**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 violators. 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 Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 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 XXX 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; <https://ag.ny.gov/>.