LYONS COMPANIES

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

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

Notice of Data Breach

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

Lyons Companies ("Lyons") writes to inform you of a recent event that may affect the privacy of some of your information. While we are unaware of any actual or attempted misuse of your information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you may take to better protect against potential misuse of information, should you feel it is appropriate. We have your data because we provide insurance brokerage services to your current or former employer, <<ClientDef2(Employer Name)>>.

What Happened? On March 12, 2019, we learned of unusual activity in an employee email account. We immediately commenced an investigation into the nature of the activity. Working with third-party forensic experts, we learned that two employee email accounts were accessed without authorization. The investigation determined that one email account was subject to unauthorized access between February 4 and March 12, 2019, and a second email account was also accessed for a few hours on March 12, 2019. While the investigation was unable to confirm whether and what information, if any, was potentially accessed, we undertook a diligent review of all data within the account to determine what information was present. Because Lyons receives data from employers in furtherance of the insurance services it offers, once the email review was complete, we worked diligently to determine from which employer the data came and to notify those employers. Lyons then worked with the relevant employers to determine contact information for those individuals whose data was present in the affected emails. Based on this effort, we determined your information was present in the emails that may have been subject to unauthorized access.

What Information Was Involved? Our investigation determined the following data related to you was present in the affected emails: <<ClientDef1(Breach Details)>>.

What Are We Doing? We take this matter, and the security and privacy of information, very seriously. In addition to conducting a diligent investigation, we are reviewing our safeguards and taking steps to enhance the security of our systems to mitigate the risk of future incidents. We are also providing you with notice of this incident, as well as information and resources you may use to better protect your personal information from potential misuse, should you feel it appropriate to do so. We will also be reporting this incident to appropriate regulatory authorities.

As an added precaution, we are providing you with access to complimentary identity monitoring and services. More information on these services and how to activate may be found in the enclosed "Privacy Safeguards."

What You Can Do. Please review the enclosed "Privacy Safeguards." We also encourage you to activate in the identity monitoring services we are offering at no cost to you.

For More Information. We understand you may have questions relating to this event and this letter. If you have questions, please contact our dedicated assistance line at 1-???-???-????, Monday through Friday, 9:00 a.m. to 6:30 p.m. ET. Again, we take this incident seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Lyons Companies

PRIVACY SAFEGUARDS

Activate Your Identity Monitoring

In an abundance of caution, 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. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To activate:

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until ***<<Date>>*** *to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

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 and to detect errors. 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 or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below 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	**TransUnion**	**Equifax**
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 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;
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	**TransUnion**	**Equifax**
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 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; 1-877-ID-THEFT (1-877-438-4338); or 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 may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us. Lyons may be contacted by mail at Rockwood Office Park, 501 Carr Rd Suite 301, Wilmington, DE 19809.

For Rhode Island Residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-247-4400. 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 potentially impacted by this incident.

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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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.

[1] 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.