By providing this notice, Hot Line Construction, Inc. ("Hot Line") does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data incident notification statute, or personal jurisdiction.

Nature of the Data Event

In late December 2018, Hot Line became aware of unusual activity relating to certain employee email accounts. Hot Line quickly began an investigation to determine the nature and scope of the activity. On January 3, 2019, the investigation, which included working with computer forensic experts, determined that certain employee email accounts were subject to unauthorized access. The investigation ultimately confirmed this unauthorized access occurred between October 25, 2018 and November 30, 2018. Because the forensic investigation could not rule out access to emails in the account during this time frame, Hot Line undertook a comprehensive review of all of the emails that were present in the relevant accounts at the time of the incident to identify what information was stored within the emails and to whom that information relates. Although the investigation found no evidence of any actual or attempted misuse of information, the review determined that the following personal information related to California residents was contained in the email accounts at the time of the unauthorized access: name, Social Security number, driver's license and financial account number.

Notice to California Residents

Hot Line began providing written notice to potentially affected individuals, including approximately two thousand, ninety-three (2,093) California residents, on April 24, 2019. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering unusual activity in an employee email account, Hot Line immediately launched an investigation to determine the nature and scope of the incident, including what information may be present in the affected accounts. Hot Line forced a password reset for all email accounts and reviewed its information security policies and procedures.

Hot Line is providing impacted individuals with access to 24 months of free credit monitoring and identity theft protection services through Kroll. Hot Line is also providing 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.

EXHIBIT A

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

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

Notice of Data Breach

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

Hot Line Construction, Inc. ("Hot Line") writes to notify you of an incident that may affect the privacy of some of your personal information. While, to date, we have no evidence of actual or attempted misuse of information potentially affected by this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information, should you feel it is appropriate to do so

What Happened? In late December 2018, we became aware of unusual activity relating to certain employee email accounts. We quickly began an investigation to determine the nature and scope of the activity. Working with computer forensic investigators, on January 3, 2019, we determined that certain employee email accounts were subject to unauthorized access. Our investigation ultimately confirmed this unauthorized access occurred between October 25, 2018 and November 30, 2018. Because the forensic investigation could not rule out access to emails in the account during this time frame, we undertook a comprehensive review of all of the emails that were present in the relevant accounts at the time of the incident to identify what information was stored within the emails. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your information was present in the affected emails.

What Information Was Involved? Our investigation confirmed the information present in the impacted email accounts includes your name and Social Security number. It may also have included your driver's license number and financial account information.

What Are We Doing. We take the security of the information in our systems very seriously. We have security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our email system, including resetting account passwords. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to protect your personal information, should you feel it is appropriate to do so. Additionally, we arranged to have Kroll protect your identity for 24 months at no cost to you as an added precaution.

What Can You Do. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll to receive the identity protection services we are making available to you. We will cover the cost of this service; however, you will need to enroll yourself in this service as we are not able to act on your behalf to do so.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-775-4209 (toll-free), Monday through Friday, 8:00 a.m. to 5:30 p.m., CT. You may also write to us at 9020 Brentwood Boulevard, Suite H, Brentwood, California 94513.

We sincerely regret any inconvenience this incident may cause you. Hot Line remains committed to safeguarding information in our care and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Lacey Harston

Lacey Harston
Director of Risk Management and Safety
Hot Line Construction, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

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 24 months. 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 **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **July 21, 2019** to activate your identity monitoring services.*

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

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, 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 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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
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
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
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

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

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); 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 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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, 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 Internet Explorer, Chrome, Firefox, and Safari. 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.