EXHIBIT 1

By providing this notice, North American Risk Services does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

Background

Earlier this year North American Risk Services discovered suspicious emails being sent from an employee's email account. North American Risk Services quickly launched an investigation, with the assistance of a third party forensic investigator, to understand the nature and scope of the event, and whether any sensitive data was at risk. The forensic investigation confirmed that just a few email accounts were subject to unauthorized access from February 7, 2018 until March 27, 2018.

The forensic investigator then reviewed the email accounts to determine if they contained any personal information. After an exhaustive search of the impacted email accounts, which included a manual review of documents to identify information contained therein, the forensic investigator confirmed on June 27, 2018 that personal information was found within the impacted email accounts. Unfortunately, the forensic investigation firm was only able to locate addresses for a quarter of the individuals and entities whose information was stored within these accounts. North American Risk Services then undertook an extensive search of its internal records to locate the missing addresses. Due to the fact that the forensic investigation firm could not find address information for approximately seventy five percent of the potentially affected population, the process of locating addresses took a significant amount of time. Once North American Risk Services recognized the significant time and effort that would be required to locate the missing addresses, North American Risk Services decided to move forward with providing notice to the affected population whose address information was provided by the forensic investigator. Our office then worked with North American Risk Services to finalize all documents required to move forward with notice to affected individuals and businesses. North American Risk Services mailed notice letters to the affected individuals and businesses it had addresses for on August 31, 2018. Due to the states of residence of the impacted individuals and number if impacted individuals in those states, notice was not required to your office as a result of the first mailing.

Following the first wave of notice, North American Risk Services devoted significant resources to locate the missing addresses including utilizing a vendor to conduct address locator services using the individuals' Social Security numbers. These address look up activities were completed on September 7, 2018. North American Risk Services will be mailing a second wave of notice letters on October 5, 2018 in substantially the same form as the letter attached hereto as ***Exhibit A***. Between the first and second mailings, six hundred four (604) California residents are being mailed notice letters. The personal information found within the impacted email accounts includes a combination of the individuals' names and one or more of the following: Social Security number, driver's license number, financial account information, medical information, health insurance information, taxpayer/employer identification number or username and password.

Other Steps Taken and To Be Taken

North American Risk Services is offering individuals impacted by this event with access to one (1) year of complimentary credit monitoring and identity restoration services. Additionally, North American Risk Services 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. North American Risk Services is also taking steps to mitigate the risk that an event like this will happen again by reviewing its policies and procedures and implementing additional email security mechanisms. In addition to providing this notice to your office, North American Risk Services is providing notice to other state regulators and the consumer reporting agencies, as required.

EXHIBIT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

RE: Notice of Data Breach

Dear <<Name 1>>:

North America Risk Services, Inc. ("NARS") is writing to notify you of a recent data security incident that may impact your personal information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft and fraud should you feel it is appropriate to do so. NARS is a third-party claims administrator and likely obtained your information due to claims management services we provided.

What Happened? Earlier this year NARS discovered suspicious emails being sent from an employee's email account. NARS quickly launched an investigation, with the assistance of a third party forensic investigator, to understand the nature and scope of the event, and whether any sensitive data was at risk. The forensic investigation confirmed that just a few employee email accounts were subject to unauthorized access from February 7, 2018 until March 27, 2018 some of which were accessible for much less time. The forensic investigator then reviewed the email accounts to determine if they contained any personal information. On June 27, 2018, NARS determined the affected email accounts contained information relating to you. Unfortunately, the forensic investigator was only able to locate a small percentage of the addresses for the individuals and entities whose information was stored within these emails. NARS then undertook an extensive search of its internal records and a third-party vendor was retained to locate the missing addresses. Once these addresses were found, NARS finalized all documents required to move forward with notice to affected individuals and businesses, including you.

What Information Was Involved? NARS cannot confirm if your personal information was actually accessed by an unauthorized actor. However, it was determined that the following information about you was accessible to the unauthorized actor: your name<<Data Elements>>.

What We Are Doing? While NARS has no indication that any fraud has or will result from this incident, we take the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we are working to implement additional safeguards and employee training in response to this incident. In an abundance of caution, we are offering you access to 12 months of credit monitoring and identity theft restoration services at no cost to you through Epiq.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Engagement Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

What You Can Do. You can enroll in the services being offered to receive free credit monitoring and identity restoration services. You can also review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." In addition, we advise you to report suspected incidents of identity theft to local law enforcement or the Attorney General.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call our dedicated assistance line at **877-327-1187**, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time as we have professionals available to answer your questions.

NARS takes the privacy and security of the personal information in our care seriously. We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

Patrick Fletcher

Patrick Fletcher
Chief Information Officer
North American Risk Services, Inc.

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

We advise you to remain vigilant by reviewing all account statements and monitoring free credit reports. We encourage you to enroll in the credit monitoring services we are offering, at no cost to you, as we are not able to act on your behalf to enroll you in the credit monitoring service. There are additional steps you can take to protect your identity should you feel it is appropriate to do so.

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 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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 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.

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, 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 9 Rhode Island residents impacted by this incident.