EXHIBIT 1

By providing this notice, Pacific Specialty Insurance Company ("Pacific Specialty") does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

Nature of the Data Security Incident

On June 14, 2019 Pacific Specialty became aware of a pattern of suspicious activity relating to certain Pacific Specialty employee email accounts. In response, Pacific Specialty worked with third party specialists to investigate the nature and scope of the activity. Through this investigation, Pacific Specialty determined that certain Pacific Specialty-managed email accounts were accessed by an unauthorized actor between March 20 and March 30, 2019. Pacific Specialty did not determine whether information stored in the email accounts was viewed or acquired by the unauthorized actor. However, Pacific Specialty could not rule out the occurrence of such activities. Therefore, Pacific Specialty performed a thorough review of the information contained within the potentially-impacted email accounts, and on November 7, 2019 Pacific Specialty became aware of the identities of the individuals whose information was contained within the impacted accounts. Pacific Specialty worked to find contact information for impacted individuals to ensure those impacted individuals received notice of this event. On January 14, 2020 Pacific Specialty confirmed the number and identities of California residents whose personal information may have been impacted. The types of personal information impacted vary by individual. However, Pacific Specialty's investigation determined that names, Social Security number, Driver's license number and other government issued identification number, financial account number, medical information, payment card number, health insurance information, username and password, relating to two thousand three hundred twelve (2,312) California residents were impacted by this incident.

Notice to California Residents

Pacific Specialty began providing written notice of this incident to two thousand three hundred twelve (2312) California residents on January 24, 2020, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Pacific Specialty investigated to determine those individuals who were affected, and secured the compromised email accounts by updating passwords.

Pacific Specialty continues to take additional steps to improve security and better protect against similar incidents in the future.

As an added precaution, Pacific Specialty is offering impacted California residents' access to twelve (12) months of free credit monitoring and identity protection services through TransUnion.

Pacific Specialty is also providing impacted California residents with guidance on how to better protect against identity theft and fraud. Such guidance includes information on how to place a fraud alert and security freeze on one's credit file, contact details for the national consumer reporting agencies, information on how to obtain a free credit report, reminders to remain vigilant for incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and recommendations regarding how to contact the Federal Trade Commission, and the State Attorney General, to report attempted or actual identity theft and fraud.

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>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

The Pacific Specialty Insurance Company ("Pacific Specialty") is writing to notify you of a recent incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On June 14, 2019 Pacific Specialty became aware of a pattern of suspicious activity relating to certain Pacific Specialty employee email accounts. In response, Pacific Specialty changed the employee's account password and worked with an outside forensics expert to investigate the nature and scope of the activity. The investigation determined that certain Pacific Specialty email accounts were accessed without authorization between March 20, 2019 and March 30, 2019. The period of unauthorized access varied for each account at issue. Every potentially accessible file within the impacted accounts was reviewed to determine what files may have been accessible to the unauthorized actor. On November 7, 2019 we became aware of the identities of the individuals whose information was included in the impacted accounts. We continued working to obtain contact information for impacted individuals through January 14, 2020.

What Information was Involved? The investigation determined that your name and <<Breached Elements>> may have been accessible by the unauthorized actor. Although this information may have been accessible, there is no indication that this information was actually viewed by an unauthorized actor. However, we are notifying you of this incident in an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among Pacific Specialty's highest priorities. Upon learning of the event, we investigated to determine those individuals that were affected, and secured the compromised accounts by changing password and enabling multi-factor authentication on all email accounts. We will be taking additional steps to improve security and better protect against similar incidents in the future.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains information on what you can do to better protect against possible misuse of your information.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive. 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 <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.

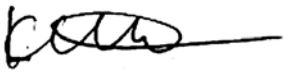
If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass 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.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please call 833-991-1528 Monday through Friday 8:00 AM to 8:00 PM (Central).

Sincerely,



Kara Holzwarth

Pacific Specialty Insurance Company

Steps You Can Take to Protect Against Identity Theft and Fraud

In addition to enrolling in the above offered services, 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**
P.O. Box 9554	**P.O. Box 160**	**P.O. Box 105788**
Allen, TX 75013	**Woodlyn, PA 19094**	**Atlanta, GA 30348-5788**
1-888-397-3742	**1-888-909-8872**	**1-800-685-1111**
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	**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	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-alerts	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.

For New York residents, the New York Attorney General provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General can be contacted by phone at 1-800-771-7755, toll-free at 1-800-788-9898, and online at www.ag.ny.gov.

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.

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 0 Rhode Island residents impacted by this incident.