EXHIBIT 1

By providing this notice, The Society does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

Following receipt of reports of potential unusual activity related to its online payment portal, The Society immediately launched an investigation, with the assistance of a third-party forensic firm, to determine the nature and scope of the activity. The third-party investigation identified suspicious code on the online payment portal on July 24, 2020. On or about July 24, 2020, the forensic investigation determined that customer payment card information processed on the website between April 16, 2020 and June 12, 2020 may have been subject to unauthorized access and/or acquisition. While the investigation was unable to definitively confirm whether any specific payment card data was accessed or taken, The Society is notifying individuals in an abundance of caution because the Society confirmed that their payment card was used on its website in the relevant time period, and their information may be affected.

The information potentially affected includes name, payment card number, expiration date, and card security code number or CVV.

Notice to Maine Residents

On or about October 7, 2020 The Society provided written notice of this incident to affected individuals, which includes three (3) Maine 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, The Society moved quickly to investigate and respond to the incident, assess the security of The Society systems, and notify potentially affected individuals. The Society is also working to implement additional safeguards and training to its employees.

Additionally, The Society 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. The Society 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.

EXHIBIT A

American Institute for Chartered Property
Casualty Underwriters / Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

The Institutes®
CPCU Society

October 7, 2020

[redacted]

B-14

Re: Notice of Data Breach

Dear [redacted]:

The Society of Chartered Property Casualty Underwriters ("The Society") recently discovered an incident that may affect the security of your payment card information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. We take this incident seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? Following receipt of reports of potential unusual activity related to its online payment portal, The Society immediately launched an investigation, with the assistance of a third-party forensic firm, to determine the nature and scope of the activity. The third-party investigation identified suspicious code on the online payment portal on July 24, 2020. On or about July 24, 2020, the forensic investigation determined that customer payment card information processed on the website between April 16, 2020 and June 12, 2020 may have been subject to unauthorized access and/or acquisition. While the investigation was unable to definitively confirm whether your specific payment card data was accessed or taken, The Society is notifying you in an abundance of caution because we have confirmed that your payment card was used on our website in the relevant time period, and your information may be affected.

What Information Was Involved? The information potentially affected includes your name, payment card number, expiration date, and card security code number or CVV.

What We Are Doing. We take this incident and the security of your personal information seriously. The Society identified the issue and moved quickly to secure the payment portal. We are also taking additional actions to enhance the security of our website portal.

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. Any suspicious activity on your financial statements should be promptly reported to the financial institution that issued your payment card. Please review the enclosed "Steps You Can Take to Protect Your Information" for additional guidance.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at 1-855-878-8555, 8:00 A.M. to 5:00 P.M. EST, Monday through Friday (excluding US holidays).

We apologize for any inconvenience or concern this incident causes you.

Yours sincerely,

Jeffrey Scheidt
Senior Vice President & Chief Financial Officer of The Institutes
The Society of Chartered Property Casualty Underwriters

Enclosure

Steps You Can Take to Protect Your Information

Monitor Your Accounts

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 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.

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 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 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are four (4) Rhode Island residents impacted by this incident.