Glencar Underwriting Managers Inc.
825 Park Boulevard
Suite 825
Itasca, Illinois 60143

March 14, 2022

[NAME]
[ADDRESS]

Notice of Cyber-Security Incident and Possible Data Exposure

The purpose of this communication is to notify you of a Cyber-Security incident involving E-Mail communications within our organization. A message containing the image of a check you used to pay an insurance premium may have been accessed by an unauthorized third party. Although we are unaware of any actual misuse of your information, we are providing notice to potentially affected organizations and individuals.

What Happened?
In April 2021 we became aware that the Company E-Mail account of one individual in our organization had been accessed by an unauthorized third party. Information in the account's mailbox was used to attempt a fraudulent financial transaction involving a business partner organization. When the attempted fraud was detected, the effected account was immediately suspended and the information in the account secured.

What Information Was Involved?
The E-Mail box that was compromised contained the scanned image of a check used to pay property and casualty insurance premiums. The check number is 116. The check itself is not dated. However, the invoice due date is 4/21/2019.

What Are We Doing?
We immediately performed an investigation to determine the extent of the unauthorized access, determine what information was accessed or exposed, and find and secure the source of the penetration. That investigation determined there is no evidence of penetration beyond the single Microsoft 365 account compromised in the initial attack. Exposed data has been identified, and all information is now secure. All required legal and regulatory reports and filings have been made, and we are notifying potentially affected individuals and organizations.

What You Can Do?
As we believe the purpose of the attack was to gather the inside business information to attempt fraudulent financial transactions and not for purpose of identity theft, we believe that the individual risk associated with the incident is low. However, we recommend that you regularly review the exposed account for evidence of fraudulent activity.

Who Can You Contact?
If you suspect fraud, immediately contact the appropriate regulatory and law enforcement authorities. If you have additional questions concerning the incident you may send us E-Mail at CPReport@gc-ins.com or leave a message containing your contact information at +1 800 221 1076. One of our representatives will respond to your request.