December 11, 2018

VIA FEDERAL EXPRESS
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Office of the Attorney General:

COR Clearing LLC ("COR") is writing to report a security incident affecting one (1) identified New Hampshire resident.

Summary of Security Incident

On September 7, 2018, COR discovered that a bad actor had used a COR employee's email account to send several "phishing" emails during the course of approximately one hour. As a result, COR commenced a forensic investigation and identified certain unauthorized logins to the email accounts of certain COR employees. On or about November 13, 2018, COR discovered the personal information of a certain New Hampshire resident in attachments to emails included in the scope of the investigation.

By obtaining access to email accounts that contained an attachment containing the personal information, it is possible that a bad actor was able to view the attachment and any personal information contained therein.

That said, based on our investigation to date, we do not have any reason to believe that the bad actors actually accessed any emails or attachments that contained personal information. In addition, COR has received no complaint from any third party suggesting that their information was obtained or misused as a result of this matter. However, because the investigation suggests that access or acquisition of content in the mailboxes was technically feasible, out of an abundance of caution, COR has elected to notify any individuals whose sensitive personal information may have been in one of the impacted email accounts.

Our Response to the Security Incident

COR engaged a cybersecurity firm to investigate the incident and conduct a forensic assessment of the incident. We also reported the incident to the FBI's Internet Crime Complaint Center, the Financial Industry Regulatory Authority, Inc. (FINRA), and the New York Department of Financial Services.

In addition, COR has implemented additional technical safeguards and has improved its procedures to increase the security of its email accounts. As part of our continual improvement of our security protocols, we are also reviewing our internal policies to make sure employees

are more aware and vigilant of fraudulent email campaigns and we are encouraging employees to report any suspicious activity.

Impacted Individual Notification & Identity Theft Protection

While we do not have any reason to believe that the bad actors actually accessed or acquired any emails or attachments that may have contained personal information, in an abundance of caution, COR will mail notification of the incident to the New Hampshire resident. The notice to includes information about how to access complimentary identity theft and credit monitoring services.

Attached please find a copy of the notification letter that will be mailed to the one (1) New Hampshire resident on December 12, 2018.

If you have any questions regarding this incident or if you desire further information or assistance, please visit https://www.corclearing.com/ or contact us at 402-836-0850. You can also email us at Ethan.McComb@corclearing.com.

Sincerely,

Ashley Randall
Compliance Officer

[RECIPIENT]
[STREET ADDRESS 1]
[STREET ADDRESS 2]
[CITY, STATE ZIP]

December _, 2018

NOTICE OF SECURITY INCIDENT

Dear [RECIPIENT],

We are writing to inform you that COR Clearing LLC ("COR") has identified certain unauthorized logins to a small number of employee email accounts that may have contained your personal information in an email or attachment.

We have not found any evidence that your personal information was accessed, acquired, or misused. However, because such access or acquisition would have been technically feasible, we are writing to you out of an abundance of caution.

We take the privacy and protection of your information very seriously, and we recommend that you review the information provided in this letter for some steps that you may take to protect yourself against the potential misuse of your information.

What Happened?

On September 7, 2018, COR discovered that a bad actor had used a COR employee's email account to send several "phishing" emails during the course of approximately one hour. Thereafter, COR discovered a small number of employee email accounts may have been accessed by a bad actor.

By obtaining access to a small number of COR email accounts that contained one or more emails or attachments containing your personal information, it is possible that the bad actors were able to view such emails or attachments and any personal information contained therein. That said, based on our investigation to date, we do not have any reason to believe that the bad actors actually accessed any emails or attachments that contained your personal information. In addition, COR has received no complaint from any third party suggesting that their information was obtained or misused as a result of this matter.

What Information Was Involved?

Based on our internal investigation, it appears that a small percentage of emails with file attachments contained personal information, including: Social Security numbers, Driver's License numbers, and/or financial account information. We note that your personal

information does not feature prominently within the impacted email inboxes and that it would generally be time-consuming for a bad actor to locate and identify such information.

What Are We Doing?

We are conducting a thorough internal forensic investigation and are working to ensure that we have robust policies and systems in place that are designed to prevent future phishing attacks. The FBI has also been notified.

What Can You Do?

As a precaution, we recommend that you take steps to guard against identity theft or fraud, generally. You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity, as further explained in the attached document. If you discover any suspicious or unusual activity on any of your financial accounts, be sure to report it immediately.

In addition, we are offering a complimentary two-year membership in Experian's IdentityWorks®. This product provides identity detection and identity theft resolution services. A credit card is **not** required for enrollment in IdentityWorks®. To activate your membership, please follow the steps below:

- Ensure that you **enroll by**: **March 31, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **insert code**

If you have questions about the Experian IdentityWorks product, you may contact Experian's customer care team at **(877) 890-9332** by **March 31, 2019.** Be prepared to provide engagement number XXXX as proof of eligibility for the identity restoration services by Experian.

In addition to Experian IdentityWorks, Experian will also provide you with identity restoration support for two years from the date of this letter. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(877) 890-9332**. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this identity restoration service does not require any action on your part at this time.

The Terms and Conditions for Experian's services are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

For More Information

If you have any questions regarding this incident or if you desire further information or assistance, visit https://www.corclearing.com/ or contact us at 402-836-0850. You can also email us at Ethan.McComb@corclearing.com

We assure you that COR takes this issue very seriously and is working diligently to ensure that this does not occur again.

Sincerely,

Ashley Randall
Compliance Officer

Information About Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

IF YOU ARE AN IOWA RESIDENT:
You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
http://www.doj.state.or.us/