17790

Portola Partners
1550 El Camino Real, Suite 200
Menlo Park, CA 94025
650-433-8779

October 6, 2020

Notice Regarding Cybersecurity Incident

Dear <<Client Name>>,

We are writing to share information with you about an email phishing incident that may have affected your personal information, steps we have taken in response to the incident, and recommended actions you may wish to take as a result. We have no evidence that your personal information was taken or misused, but we are unable to rule out the possibility that some information about you may have been compromised. We see no scenario where any of your usernames or passwords would have been compromised because of this incident. This phishing attack solely compromised a single Portola Partners ("Portola") employee's computer and in no way compromised the integrity of the Portola platform.

In the spirit of transparency and to satisfy regulatory requirements, we are providing you with this notice, which includes language required by regulators. <<Advisor>> hopes to speak with you as soon as practical to answer any questions. We sincerely apologize for any concern or inconvenience.

What Happened?

On September 8, 2020, Portola was alerted to the potential compromise of the computer of one of our employees. We promptly identified malware on the employee's computer, quarantined the malware, and began a forensic investigation into the source and impact of the malware. We determined that the malware was delivered to the impacted computer in a reply to a pre-existing email thread from a compromised email account belonging to a client's bookkeeper. This email came from a real email account, was a response on an existing email chain, and had an embedded link where a link was expected. Because we had multi-factor authentication enabled, the malware was not able to perpetuate beyond the employee's computer. No other employee computers or Portola systems were impacted. The malware is designed to steal online account usernames and passwords, and it has the capability to take screen shots or video of its victim's computers. Importantly, to our knowledge, we do not possess any usernames or password for your accounts. Moreover, as you know, Portola employees are unable to authorize transactions in your accounts.

While we do have evidence that the malware was active, we do not have evidence 1) that the above-mentioned capabilities were initiated, 2) that any information was taken out of our systems, 3) that there was financial fraud with any Portola accounts, including yours, or 4) that there was any other misuse of data. Nevertheless, given the malware's capabilities, we are unable to rule out the possibility that some information about you may have been compromised. Hence, in the spirit of transparency and to satisfy regulatory requirements, we are providing this notice because your personal information may have been available through the impacted computer.

What Information Was Involved?

The impacted computer had access to client account information (including client account names or pseudonyms, social security numbers, bank account and routing numbers, dates of birth), government issued identification numbers (such as passport or driver's license information), and investment strategies.

What We Are Doing.

Upon discovery of this incident, we immediately investigated, contained, and remediated the impacted computer. We informed the client's bookkeeper from whom the malware originated. We have spoken about

his incident with both Fidelity and Schwab to ensure that our clients' accounts are appropriately secure. We have also notified federal and appropriate state law enforcement agencies. If you would like, we would be happy to set up credit monitoring services for ten years at our expense.

What You Can Do.

Although there is no indication that any Portola client information has been misused, we encourage you as always to regularly review your financial accounts and credit reports for any suspicious activity. Report any suspected incidents of fraud to the relevant financial institution. We also have included an attachment listing additional steps you may wish to consider taking if you ever suspect that you may have been the victim of identity theft. We offer this information in case it may be helpful to you.

We take the security of your information very seriously. We truly regret and apologize for any concern or inconvenience this incident may cause you. If you have any questions or concerns, please do not hesitate to contact me at 650-289-1114 or srehmus@portolapartnersllc.com.

With sincere apologies,

Steve Rehmus

Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

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 at 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, GA 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**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1-800-916-8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1-800-766-0008
Experian:	Report Fraud:	1-888-397-3742
TransUnion:	Report Fraud:	1-800-680-7289

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a customer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00 (or in certain states no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified, or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.)
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill

- A photocopy of a government-issued ID card
- 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
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express, or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include: (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W. Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, and any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.
- Oregon residents report to state Attorney General. Oregon residents who suspect they have been the victim of identity theft should file a report with the Oregon Attorney General at 877-877-9392.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W. Washington, D.C. 20580.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at https://ncdoj.gov/protecting-consumers/protecting-your-identity/, calling 919-716-6000, or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service, Raleigh, NC 27699-9001.