CORPORATION

211 Main Street
San Francisco, CA 94105
Main (800) 435-4000

Sent via Overnight Mail

May 3, 2016

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Attorney General Joseph Foster

We are writing to notify you that Charles Schwab & Co. Inc. ("Schwab") recently discovered unusual login activity on the Schwab accounts of certain New Hampshire residents. We believe this activity resulted from what is known as a "Credential Replay" incident, in which criminals use an automated program to test large numbers of login credentials against many different accounts, hoping to achieve coincidental matches. While it is unclear exactly what Schwab account information was accessed by the person or persons who carried out this effort, as a precautionary measure we have decided to notify all affected New Hampshire residents and your office. Schwab's own computer systems were not compromised in this incident, and Schwab is not aware of how or from what other site the credentials were obtained.

NATURE OF UNAUTHORIZED ACCESS

Schwab began an investigation into unusual login activity in mid-April, and while the investigation is ongoing, we believe that on or after March 25, 2016, someone unlawfully obtained the usernames and passwords of New Hampshire residents from a non-Schwab account or website and tried them successfully on Schwab.com. This type of Credential Replay incident is made possible when clients use the same username and password on multiple sites. Schwab accounts provide online access to clients' names, account numbers, and other information about their investment strategy, including positions and transaction activity. However, it is not clear whether any of the information available on schwab.com was actually accessed through a coincidental match through the automated Credential Replay.

NUMBER OF RESIDENTS AFFECTED

18 New Hampshire residents were affected by this incident. We are notifying residents by email or regular mail and requiring them to re-set their passwords. A sample client communication, which will be sent on or about May 4, 2016, is attached for your reference. We continue to monitor our systems for suspicious log-ins, are reminding customers about good password practices, and if the Credential Replay activity continues, we will continue to notify affected residents and require them to change their password.

ADDITIONAL STEPS BEING TAKEN BY THE COMPANY

After discovering the issue we restricted online account access until we could speak with each affected account holder. We have been actively monitoring the accounts for suspicious activity. We are attempting to contact each resident by phone in order to verify their identity before re-establishing online account access and to discuss steps we suggest they take to protect themselves and their accounts. We have also notified the Federal Bureau of Investigation and our primary federal regulators.

CONTACT INFORMATION

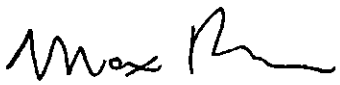
If you have any questions or need additional information, please contact me:

Max Ruston

415-667-1511

max.ruston@schwab.com

Sincerely,



Max Ruston

Corporate Privacy Officer

charles SCHWAB

NOTICE OF UNUSUAL LOGIN ACTIVITY

May 4, 2016

What Happened?

We are contacting you to alert you to unusual login activity on your account(s), which began on or after March 25, 2016. We believe someone may have obtained your username and password from a non-Schwab account or website that you use and tried them successfully on Schwab.com. This type of account access can occur when you use the same username and password on multiple sites.

Although we have no indication that your holdings have been impacted as a result of this access, we encourage you to review your financial accounts and credit reports, remain vigilant for the next 12 to 24 months, and report any suspicious or unrecognized activity immediately to local law enforcement and your financial institution(s).

What Information Was Involved?

Schwab accounts provide online access to clients' names, Schwab account numbers, and other information, including positions and transaction history. The fact that such information is available on Schwab.com does not necessarily mean that your information was accessed by the person(s) who used your login credentials. This is because the person(s) involved likely used an automated program to test large numbers of login credentials against many different accounts, both at Schwab and likely at other financial institutions. The fact that this effort yielded a number of coincidental matches, including for your account(s), does not necessarily mean that your account information was accessed.

What We Are Doing.

After we discovered the issue, to protect your confidential information, we restricted your online account access until we could speak with you. We have also been actively monitoring your account for suspicious activity.

We are attempting to contact you by phone, or if you are a client of an independent investment advisor, we have asked your advisor to contact you. By the time you receive this email, a Schwab representative or your advisor may already have spoken to you and explained the steps we recommend you take.

What You Can Do.

If you haven't spoken with a Schwab representative yet, please call us so we can re-establish your online access and discuss other actions you might want to take.

The security of your account is important to us. Please call us at 877-903-1570 or at one of the contact numbers on our website or on your Schwab account statements.

Other Important Information

Credit Reporting Agencies

Equifax P.O. Box 740241 Atlanta, GA 30348 Phone: 866-493-9788	TransUnion P.O. Box 2000 Chester, PA 19022 Phone: 800-680-7289	Experian P.O. Box 4500 Allen, TX 75013 Phone: 888-397-3742

If you believe you have been the victim of identity theft, you should report that to your local law enforcement agency and consider contacting the above credit reporting agencies to place a "fraud alert" or "security freeze" on your credit file, which will notify lenders to verify your ID before extending credit in your name. You may need to provide them with a police report, and each agency may charge you up to $10. Instructions for requesting a free copy of your credit report can be viewed at https://www.consumer.ftc.gov/articles/0155-free-credit-reports.

You can contact the Federal Trade Commission to learn more about how to protect yourself from identity theft. Write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington, DC 20580; call 877-FTC-HELP (877-382-4357); or visit their website at https://www.identitytheft.gov/info-lost-or-stolen.

Some states provide other resources for their residents:

Iowa Residents: You can also report suspected incidents of identity theft to local law enforcement or the Office of the Iowa Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319; 515-281-5164; http://www.iowaattorneygeneral.org.

Maryland Residents: To obtain more information about steps you can take to avoid identity theft, you can contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 888-743-0023; www.oag.state.md.us/contact.htm; or the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington, DC 20580;

Massachusetts and West Virginia Residents: Applicable law requires that we notify you that you can also place a security freeze on your credit report to prevent potential credit grantors from accessing your credit report without your consent, by sending a written request to each of the national credit reporting agencies listed above. In order to request a security freeze, you will need to provide the following: (1) your full name, with middle initial and any suffixes; (2) your Social Security number and date of birth; (3) proof of your current address, such as a utility or phone bill, as well as a list of your addresses from the prior five years; (4) a legible photocopy of a government-issued identification card; (5) if you have been a victim of identity theft, a copy of any police report, complaint, or other investigative report you may have filed with local law enforcement; and (6) if you are not a victim of identity theft, payment by check, money order, or credit card. Do not send cash. The credit reporting agency may charge a fee of up to $10 each to place, temporarily lift, or remove a freeze. To lift or remove a freeze, you must send a written request in accordance with the requirements of each credit reporting agency. 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 credit, loans, employment, housing, or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly. Under state law, you also have the right to request a copy of any police report filed in connection with this incident.

North Carolina Residents: To obtain more information about steps you can take to avoid identity theft, you can contact the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (877-566-7226); www.ncdoj.gov; or the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington, DC 20580; 877-ID-THEFT (877-438-4338); https://www.identitytheft.gov/info-lost-or-stolen.

Oregon Residents: You can also report suspected incidents of identity theft to law enforcement or to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington, DC 20580; https://www.identitytheft.gov/info-lost-or-stolen.

Vermont Residents: You can learn helpful information about fighting identity theft, placing a security freeze on your credit file, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.