

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K STREET, NW
TELEPHONE (202) 223-7300

WASHINGTON, DC 20006-1047

1285 AVENUE OF THE AMERICAS
NEW YORK, NY 10019-6064
TELEPHONE (212) 373-3000

UNIT 5201, FORTUNE FINANCIAL CENTER
5 DONGSANHUAN ZHONGLU
CHAORYANG DISTRICT, BEIJING 100020, CHINA
TELEPHONE (86-10) 5828-6300

SUITES 3601 – 3606 & 3610
36/F, GLOUCESTER TOWER
THE LANDMARK
15 QUEEN'S ROAD, CENTRAL
HONG KONG
TELEPHONE (852) 2846-0300

ALDER CASTLE
10 NOBLE STREET
LONDON EC2V 7JU, UNITED KINGDOM
TELEPHONE (44 20) 7367 1600

535 MISSION STREET, 24TH FLOOR
SAN FRANCISCO, CA 94105
TELEPHONE (628) 432-5100

FUKOKU SEIMEI BUILDING
2-2 UCHISAIWAICHO 2-CHOME
CHIYODA-KU, TOKYO 100-0011, JAPAN
TELEPHONE (81-3) 3597-8101

TORONTO-DOMINION CENTRE
77 KING STREET WEST, SUITE 3100
P.O. BOX 226
TORONTO, ONTARIO M5K 1J3
TELEPHONE (416) 504-0520

500 DELAWARE AVENUE, SUITE 200
POST OFFICE BOX 32
WILMINGTON, DE 19899-0032
TELEPHONE (302) 655-4410

WRITER'S DIRECT DIAL NUMBER

(202) 223-7485

WRITER'S DIRECT FACSIMILE

(202) 204-7395

WRITER'S DIRECT E-MAIL ADDRESS

pcarey@paulweiss.com

November 10, 2023

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of our client Chicago Trading Company (“CTC”), a trading firm, I am writing to inform you about a recent incident in which personal information relating to Maryland residents was accessed by an unauthorized third party. CTC’s headquarters is located at 425 S Financial Place, 4th Floor, Chicago, Illinois 60605.

Specifically, CTC was the victim of a cybersecurity incident in which a cyber criminal gained access to certain corporate systems and data on October 27, 2023. After discovering the incident that same day, CTC worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. CTC concluded that the unauthorized actor stole certain internal business documents related to CTC.

Through CTC’s investigation, the company determined that the third party accessed the name, birth dates, addresses, passport information and driver’s license information, and/or Social Security number of up to two individuals who are Maryland residents. While it is possible that some of these individuals may not have had any of this information impacted, out of an abundance of caution, CTC is notifying every individual and offering credit monitoring as described below.

Maryland Attorney General's Office

2

CTC maintains a written information security program. With professional support from third-party cybersecurity experts, CTC promptly responded to contain and investigate the incident. CTC also conducted a thorough investigation, which included our full cooperation with law enforcement. Additionally, CTC is conducting a comprehensive review and audit of its security policies including patching policies and implementing additional advanced security measures. Lastly, CTC will be making enhancements to how it protects information on its network.

CTC will notify two Maryland residents of this incident on or about November 10, 2023. CTC will provide these individuals with an offer for 24 months of complementary credit monitoring. The letter that CTC is providing to Maryland residents includes all information necessary for the residents to enroll in the Equifax Complete Premier credit monitoring service.

Attached is a copy of the letter that CTC is providing to Maryland residents.

Please do not hesitate to contact me at (202) 223-7485 if you have any questions. I also can be reached at pcarey@paulweiss.com and at the below address:

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, DC 20006-1047

Sincerely,

/s/ Peter Carey

Peter Carey
Counsel

Attachment



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>>, <<State>><<Zip>>
<<Country>>

<<Date>>

RE: **Notice of Data Breach**

Dear <<Name 1>>:

I am writing to inform you about a cybersecurity incident that involved certain personal information about you. This incident has not disrupted our operations; nevertheless, we regret that this incident occurred and take the security of all employees' personal information very seriously.

WHAT HAPPENED. CTC was the victim of a cybersecurity incident in which a criminal gained access to certain corporate systems on October 27, 2023. After discovering the incident on the same day, CTC worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. Even though our investigation is not complete, we have been able to confirm that the criminal stole and may post on the dark web certain internal business documents related to CTC.

WHAT INFORMATION WAS INVOLVED. We determined that employee Personal Identifiable Information (PII) was present in the stolen data. The types of PII include Social Security numbers, birth dates, passport information and driver's license information. While it is possible that some employees may not have had any PII impacted, out of an abundance of caution, we are notifying every employee and offering credit monitoring as described below.

WHAT WE ARE DOING. Information security is a priority for CTC. We took immediate steps in response to the incident to stop the unauthorized access and secure our systems. We also conducted a thorough investigation, which included our full cooperation with law enforcement. Additionally, we are conducting a comprehensive review and audit of our security policies including patching policies and implementing additional advanced security measures. Lastly, we will be making enhancements to how we protect information on our network and ask for your cooperation and attention when we communicate these changes.

WHAT YOU CAN DO. I understand this is concerning news and we are taking a series of steps to provide support to employees. Consistent with certain laws, we are providing you with the following information about general steps that you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary 24-month credit monitoring service. During this period, CTC will pay for Equifax to provide you with its Credit Watch Premier service, which includes, among other things, three-bureau credit monitoring, web monitoring, and identity theft protection and restoration services, including up to \$1,000,000 of identity theft insurance coverage. You have until **February 29, 2024** to activate the free credit monitoring service by using the following activation code: <<Code>>. This code is unique for your use and should not be shared. To enroll, go to www.equifax.com/activate.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institution.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s web site, www.ftc.gov/idtheft/, call the FTC at (877) IDTHEFT (438-4338), or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit-reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit-reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com/personal/credit-report-services	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 www.experian.com/help	TransUnion (888) 909-8872 Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19022 www.transunion.com/credit-help
--	--	--

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and credit freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze or restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Please know that we sincerely regret any inconvenience or worry this incident may cause you. Please do not hesitate to contact us incident.response@chicagotrading.com or via our support center at 888-983-0230 if you have any questions or concerns.

Sincerely,

Alison Potish

Chief People Officer
Chicago Trading Company

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

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

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue, Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7726
<http://www.ncdoj.com>