



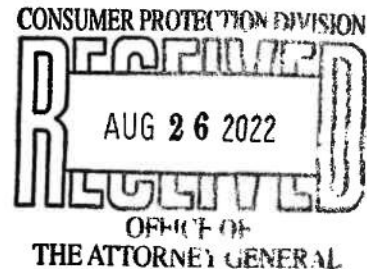
Paul F. Schmeltzer
T (213) 417-5163
F +121348811
Email:pschmeltzer@ClarkHill.com

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F +12134881178

August 12, 2022

VIA USPS:

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202



To Whom It May Concern:

We represent Midwestern Securities Trading Company, LLC ("MSTC") with respect to a data security incident involving the potential exposure of personally identifiable information described in more detail below. MSTC takes the security of information in its control seriously and has taken steps to prevent a similar incident in the future.

1. Nature of security incident.

On August 26, 2021, an MSTC employee's email address was accessed by an unauthorized person who used the email account to send phishing emails from the employee's account to all their contacts in their address book. The unauthorized person created mailbox rules that prevented the employee from noticing the sent emails and subsequent responses from those that received them. MSTC reacted quickly to implement their incident response plan and were able to terminate the unauthorized access within 15 minutes of the first email being sent. MSTC then notified the contacts in the employee's address book, and third-party vendors who could have received a phishing email, that the emails were not sent by MSTC.

It is MSTC policy that personally identifiable information sent by MSTC employees via email be done in an encrypted and secure manner. Encrypted emails were in the impacted employee's sent folder and could have been viewed by the unauthorized person. The personally identifiable information that might have been present in the encrypted emails could include a combination of name, account information, login information, and Social Security number. Out of an abundance of caution, MSTC provided written notice of the incident to the contacts in the employee's address book and third-party vendors who could have received a phishing email.

2. Number of residents affected.

(Five) (5) residents of Maryland were notified of the incident. A notification letter was sent to the affected individual on July 28, 2022 via regular mail. A copy of the form notification letter is enclosed.

3. Steps taken relating to the incident.

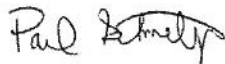
In response to the incident, MSTC performed two password resets on the impacted employee email account, and enabled multi-factor authentication on their email systems. MSTC is continuously reviewing its security posture to ensure appropriate controls are in place. Impacted individuals were also offered 12 months of credit and identity theft monitoring services through Norton LifeLock.

4. Contact Information.

MSTC remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (323) 497-4493 or pschmeltzer@clarkhill.com

Very truly yours,

CLARK HILL



Paul Schmeltzer

Enclosure



Midwestern Securities Trading Company, LLC
P.O. Box 2528, East Peoria, IL 61611
309.271.7322

Recipient Name

Address

City, State ZIP

Notice of Data Notice of Data Security Incident

We are writing to inform you of a data privacy incident experienced by Midwestern Securities Trading Company, LLC that may have resulted in unauthorized access to your personal information, including your name, account information, and Social Security number. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you.

What Happened:

We became aware of unusual activity relating to certain company systems and promptly investigated. That investigation found that your information was stored on a system affected by the incident. The investigation, unfortunately, could not determine whether any of that information had been accessed or removed during the incident, only that it was present. And so, out of an abundance of caution we are providing you with notice of this incident.

What Information was Involved:

A thorough review of the system contents determined that, at the time of the incident, the affected systems contained information that may have included your name, account information, and Social Security number.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this kind of event from happening in the future. Information, privacy, and security are among our highest priorities. As such, upon learning of this incident we quickly investigated and confirmed the systems' security. In an abundance of caution, we also promptly disabled access to the affected systems, implemented increased security measures, conducted additional employee training, and are currently and regularly reviewing our policies and procedures relating to data security.

What You Can Do:

We believe it is unlikely that any of your information will be misused. That said, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) months. We also encourage you to enroll with an identity and credit monitoring service, such as Credit Sesame, Credit Karma, Experian, or Norton LifeLock. Please note that you must enroll directly, as we are unable to enroll in these services for you.

More Information:

If you have additional questions about the incident, please call 309-271-7322. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Midwestern Securities Compliance Department

Recommended Steps to Help Protect Your Identity

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud
Reporting and Credit
Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Residents can report suspected incidents of identity theft to local law enforcement or the attorney general: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, or visit <https://www.iowaattorneygeneral.gov/contact-us>.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft