

December 16, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

By (Secure) Email:
ldtheft@oag.state.md.us

To whom it may concern:

On behalf of Citigroup Global Markets Inc. ("CGMI"), this is to inform you that an unauthorized actor, apparently having acquired certain clients' username(s) and password(s) via an unrelated event outside of CGMI systems, used those credentials in an automated credential stuffing event through a third party's website in an attempt to link clients' CGMI brokerage account to said third party site. The actor temporarily accessed limited data including certain client account numbers and limited account information regarding balances, transaction history and positions on or about November 1, 2024. Such access was detected and immediately terminated on that same date. As described in the attached notice, we initiated an investigation as soon as we learned of these issues to assess and remediate the incident and limit its effect; continue to use ongoing measures to protect accounts and personal information; with the client reset applicable access codes; and have disabled the service used to connect to clients' external service provider.

As a precaution, we have arranged for the person associated with the account at their option to enroll in a credit monitoring subscription at no cost to them for not less than twelve (12) months. Five (5) Maryland client residents will be sent the attached letter of a total three hundred and forty clients related to the event receiving a similar notice. We take very seriously the security of personal information and bring this notice and action to your attention. Attached is a sample of the letter that we are providing to your state residents.

Please do not hesitate to contact me if you have any questions or need additional information.

Sincerely,
Dan McElwee
Associate General Counsel
Citigroup Global Markets Inc.
388 Greenwich Street
New York, NY 10013
Phone: (718) 248-3230
E-mail: dan.mcelwee@citi.com

Attachment (below): Notice Template 2024-0053069.0048254US.02



NOTICE OF SECURITY INCIDENT

[DATE] 2024

Name & Address

Re: Your Citigroup Global Markets Inc. Brokerage Account Ending in [...xxx] – Security Notice

Dear [Name],

On behalf of Citigroup Global Markets Inc. (CGMI), we are writing to inform you about a recent incident that involved your personal information.

WHAT HAPPENED

We recently discovered that an unknown person posing as your service provider used your User ID and Password (“username and password”) for the NetXInvestor® web site at Pershing LLC (“NetX”) to temporarily access NetX to acquire limited information about your CGMI brokerage account. Your credentials appears to have been obtained outside of CGMI possibly from a location or site where you used them for similar or other purposes. Limited brokerage account information was temporarily accessed through the NetX site before Pershing terminated the connection. **The actor did not access your brokerage account directly and was not able to perform any actions in your account.**

We take the security of your personal information very seriously. You should **promptly change the username and password** for the NetX site and **anywhere else you might use them**. As a measure of caution, we have arranged for you, at your option, to enroll in a credit monitoring service described below. We also want to apologize for any inconvenience this may cause you.

WHAT INFORMATION WAS INVOLVED

Through our investigation, we have determined that the unauthorized actor using your username and password acquired temporary access to limited information about your brokerage account on or about *[insert date related to above noted account(s)]* that included your account number, and certain balance, position, and transaction information.

WHAT WE ARE DOING

We initiated an investigation as soon as we learned of these issues to assess and remediate the incident and limit its effect on you. We continue to use ongoing measures to protect your account and personal information. As you may know, the service used to connect NetX to your external service provider has been disabled by Pershing at our request.

WHAT YOU CAN DO

As a precaution, you should change your NetX username and password for your account. **The credentials must be reset by you.** You can reset your credentials online by following the prompts at <https://investments.citi.com> or by contacting us through your account representative or at the Citi contact number below. We also strongly recommend that you **promptly cancel and change that username and password anywhere else you might be using them**.

In addition to the actions noted above, as a precaution, we have arranged for you at your option to enroll in **Experian's® IdentityWorks** at no cost to you for up to twelve (12) months. To activate this coverage, please call the toll-free number or visit the website, listed below and enter the Activation Code. The Activation Code is required for enrollment and is unique for your use and should not be shared. You will also need to provide your Social Security Number to enroll.

Activate Experian's® IdentityWorks in Three Steps:

1. Ensure that you enroll by [Date] (Your code will not work after this date).
2. Web Site: Visit the IdentityWorks web site to enroll: <https://www.experianidworks.com/3bplus>
3. Provide your Activation Code: [#X#]

If you have enrollment questions or need an alternative to enrolling online, please call 1-877-534-7033 and provide engagement number: <engagement number.>

FOR MORE INFORMATION.

If you have questions or concerns about this, or if we can be of further assistance to you, please do not hesitate to **contact us** at **National Investor Center at 1-877-357-3399**. We have also included Additional Information about protecting your identity below.

Sincerely,
Citigroup Global Markets Inc.

ADDITIONAL INFORMATION

This incident did not involve your credit and should not affect your account going forward. However, the following general tips may be helpful in monitoring and protecting your information.

- You should regularly review your account statements and monitor free credit reports. Please promptly report suspicious or unusual activity on your accounts to us.
- Under federal law, you are entitled to obtain one free copy of your credit report every twelve months from each of the nationwide consumer reporting agencies. You can obtain a free copy of your credit report from each agency by calling 1-877-322-8228 or visiting www.annualcreditreport.com. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you may request that the credit reporting agency delete that information from your credit report file.
- Consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account but might also delay any requests you might make for new accounts.
 - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105069, Atlanta, GA 30348-5069
 - Experian: 1-888-EXPERIAN (397-3742); experian.com/fraud; P.O. Box 9532, Allen, TX 75013
 - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- To report incidents of fraud and identity theft, you can contact the Federal Trade Commission (FTC) at 1-877-ID-THEFT, through their website at <http://identitytheft.gov> or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20850. You can also contact local law enforcement or your state's attorney general.

OTHER IMPORTANT CONTACT INFORMATION

IF YOU ARE A MARYLAND RESIDENT: You may also 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.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may also 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
9001 Mail Service Center, Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE AN RHODE ISLAND RESIDENT: You may also obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at: Rhode Island Office of the Attorney General

150 South Main Street, Providence, RI 02903
Phone: (401) 274-4400
<http://www.riag.ri.gov>

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection. This office can be reached at: New York State Division of Consumer Protection

123 William Street
New York, NY 10038-3804
1 (800) 697-1220
One Commerce Plaza,
99 Washington Ave.
Albany, NY 12231-0001
<http://www.dos.ny.gov/consumerprotection>

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may also obtain information about preventing identity theft from the D.C. Attorney General's Office. This office can be reached at: Office of Consumer Protection

441 4th Street, NW, Washington, DC 20001
(202) 442-9828
<https://oag.dc.gov/consumer-protection>

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive Identity Restoration support.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you would like to discuss Experian Restoration support, please reach out to an Experian agent at the Experian number noted in this letter. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent may be available to work with you. Please note that this Identity Restoration support is available to you for a limited time from the date of this letter. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this Experian site.

If you have any questions about **IdentityWorks**, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.