BANK OF AMERICA

Notice of Data Breach

Customer Name
Street Address
City, State Zip

Reference Number 2024-7942

Date

Customer first and last name:

WHAT HAPPENED: A Bank of America third-party provider discovered on October 1, 2024, that an unauthorized party gained access to their systems. The unauthorized activity on the third-party provider's systems has been stopped, and Bank of America's systems were not impacted by this event.

WHAT INFORMATION WAS INVOLVED: According to our records, the information involved in this incident was related to your mortgage loan and may have included your first and last name, address, passport number, phone number, Social Security number and loan number.

Your security is our priority. We understand how upsetting this can be and sincerely apologize for this incident and any concerns or inconvenience it may cause. We are notifying you so we can work together to protect your personal and account information.

WHAT WE ARE DOING

We have conducted our own internal investigations to prevent and minimize any financial impact to you.

- We are monitoring your accounts and will let you know if we notice any suspicious activity.
- We will work with you to resolve any unauthorized transactions on your Bank of America and / or Merrill Lynch Brokerage account(s) related to this incident if reported in a timely manner.
- We have also arranged for a **complimentary one-year membership in an identity theft protection service** provided by Experian IdentityWorks℠.
  - This service includes daily monitoring of your credit reports from the three national credit reporting agencies — Experian®, Equifax® and TransUnion® — plus internet surveillance and help with the resolution of identity theft.
  - To learn more about this membership or to enroll, go to **experianidworks.com/bac**, enter your activation code and engagement number then complete the secure online form. To enroll by phone, please call Experian IdentityWorks at 866.617.1920.

    Activation code: (Adult Activation Code)
    Engagement number: (Adult Engagement number)
    You must enroll by Month, Day, Year to take advantage of this offer.
  - This service will automatically expire at the end of the two-year period. You can renew the service and pay for it yourself by contacting Experian IdentityWorks. We have no involvement in any offers, products or services from or through them, that you choose to enroll in beyond the complimentary membership.

WHAT YOU CAN DO

Together, we can make the strongest possible defense against fraud. To help protect your account(s) and personal information:

- **Review your information**
  - As your statements arrive, promptly review them and your credit reports over the next 12 to 24 months and notify us of any unauthorized transactions, or incidents of suspected identity theft or fraud.

- **Protect your brokerage accounts**

  - We recommend you set up a Relationship Personal Identification Number (RPIN) as a secondary layer of protection for your Merrill Lynch brokerage account(s). An RPIN is a secure and simple verification method for accessing account information through our automated system or the Merrill Lynch Wealth Management contact centers. Once established, your RPIN will be required before any information is given or transaction can be processed.
  - Call 1.800.MERRILL (637.7455) and say service associate at the main menu for help creating an RPIN.
  - Please contact your Financial Advisor if you want to change your account number(s).

- **Check your contact information**
  - Keep your contact information up-to-date, especially your mobile number. If we spot an issue, we want to get in touch with you the quickest way possible so we can alert you to potential fraud or suspicious activity.
- **Create a strong unique password**
  - Strong passwords are eight or more characters long and include a combination of numbers, symbols and upper- and lowercase letters.
  - Use additional security features such as multifactor authentication when possible.
- **Keep your account information secure**
  - Guard your Social Security number, PINs, passwords and account numbers. Never write your PIN on the back of your card.
  - Go paperless and use trusted online payment methods.
- **Protect your devices**
  - Stay alert to online threats. Keep your phone, tablet and computer up to date with the latest browser, operating system and antivirus software.
  - Avoid clicking suspicious links or responding to emails or texts urging you to act quickly.

Please refer to our security center at **bankofamerica.com/security** and the *Important Tips on How to Protect your Personal Information* document we've included for additional information and precautions you can take.

FOR MORE INFORMATION

If you have any questions, please call our Privacy Response Unit at 800.252.2867, Monday through Friday, 9 a.m. to 9 p.m. Eastern.

Important Tips on How to Protect your Personal Information

We are providing you with some precautions to help safeguard against the disclosure and unauthorized use of your account and personal information.

- Review your account statements thoroughly and report any suspicious activity to us.
- Memorize your personal identification numbers (PINs) and do not write them down where they could be found.
- Report lost or stolen checks and/or cards immediately.
- Keep a list of your account numbers, along with your financial institution's contact information, in a separate, secure location.
- Do not provide personal information over the phone or online unless you have initiated the contact and know who you are speaking with.
- Do not include your driver's license or Social Security number on checks, preprinted or otherwise.
- Store checks and account statements in a safe place.
- Reduce the amount of paper you receive containing personal information by signing up for online statements, direct deposit and online pay bill services.
- Destroy or shred any pre-approved credit offers you receive.
- Change your passwords and PIN numbers every three months and monitor all your account(s), including any additional account(s) you may have with other financial institutions, to help prevent or detect any unauthorized or fraudulent activity.
- Review your credit report at least once every year. Make sure all the information is current and accurate. Report any fraudulent transactions immediately and once resolved, work with the credit reporting agencies to ensure the inaccurate information is deleted from your credit report. For a free copy of your credit report, contact **annualcreditreport.com** or call **877.322.8228**.
- Install virus and spyware detection software on your computer(s) and update them regularly.
- Download mobile apps from the appropriate vendor and ensure you update your mobile banking apps as new versions become available.
- Limit the information you share on social networking sites such as your full legal name, along with your address, date of birth, and other identifiable information.

Beware of Phishing

Beware of common phishing attempts such as mail, phone calls and emails containing typos or other errors, or when you are asked for your personal information. Examples of common scams are identity verification requests to prevent account closure or promises of financial incentive if you provide your account information.

Keep in mind, financial institutions will not request you to provide your personal information, such as Social Security number or log in credentials such as passwords or PINs.

For more information about guarding your account and personal information, as well as our online practices, please visit us online at **bankofamerica.com/privacy** or **ml.com/privacy**.

Placing, Lifting and Removing a Security Freeze on your Credit Reports

A security freeze on your credit report prohibits the credit reporting agency from releasing information from your credit report without your permission. Please keep in mind, a security freeze may delay, interfere with, or prevent the timely approval of requests made for loans, mortgages, employment, housing, or other services. Under federal law, you cannot be charged for placing or removing a security freeze.

To request a security freeze on your credit reports, send a request by mail, through their website or by phone to each of the reporting agencies using the contact information in the *Reporting Fraud* section below.

You will need to provide some or all this information to each credit reporting agency:

- Your full name
- Social Security number
- Date of birth
- Mailing addresses from the past five years
- Proof of your current address — a recent electric bill or bank statement
- A legible photocopy of a valid government issued ID card or driver's license
- Social Security card, a recent pay stub or W2
- A copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Confirmation of security freeze and PIN/Password. The credit reporting agencies have one to three business days after receiving your request to place a security freeze on your credit report. The agencies must send you a written confirmation in five business days and provide you with a unique personal identification number (PIN), a password, or both, to use for authorizing the removal or lifting of the security freeze. We recommend you keep your PIN/password in a secure place.

How to lift a security freeze. You can lift the security freeze and allow a specific entity or individual access to your credit report, or temporarily lift a security freeze for a specific period of time, by making a request to each of the credit reporting agencies by mail, through their website or by phone. You must provide proper identification and the PIN or password provided to you when you placed the security freeze, as well as the identities of the entities or individuals you would like to receive your credit report. The agencies have one hour for requests made online, and three business days for request made by mail, after receiving your request to lift the security freeze.

How to remove the security freeze. To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website or by phone. You must provide proper identification and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour for requests made online, and three business days for requests made by mail, after receiving your request to remove the security freeze.

Reporting Fraud

If you think you are a victim of identity theft or fraud, contact any of these credit reporting agencies to place a fraud alert on your file. A fraud alert will prevent new credit accounts from being opened without your permission. The agency you contact will forward the alert to the other agencies, so you do not have to contact them all.

Trans Union
PO Box 6790
Fullerton, CA 92834-6790
800.680.7289
transunion.com

Experian
PO Box 9532
Allen, TX 75013-0036
888.397.3742
experian.com

Equifax
PO Box 105069
Atlanta, GA 30348
800.525.6285
equifax.com

Also contact the Federal Trade Commission (FTC) to report any incidents of identity theft, or to receive additional guidance on steps you can take to protect against identity theft. Visit the FTC Identity Theft website at **consumer.gov/idtheft or call 877.438.4338**. **TTY: 866.653.4261**. The FTC's address is: **600 Pennsylvania Avenue, NW, Washington, DC 20580.**

Your Bank of America Accounts

Report fraudulent activity on your Bank of America accounts, or within Online Banking, to us at **800.432.1000**.

Your Merrill Lynch Accounts

Report fraudulent activity on your Merrill Lynch accounts by calling us anytime at 800.MERRILL (**637.7455**) for advisory accounts, or **877.653.4732** for Merrill Edge accounts.

You may contact your state Attorney General for additional information about avoiding identity theft.

State-specific Attorney General Contact Information:

District of Columbia Office of the Attorney General
Office of Consumer Protection
400 6th Street NW
Washington, DC 20001
202.442.9828
www.oag.dc.gov

Massachusetts Office of the Attorney General
One Ashburton Place
Boston, MA 02108
617.727.2200
www.mass.gov/orgs/office-of-the-attorney-general
Note: Massachusetts residents have the right to a copy of any police report if one was filed. If you're the victim of identity theft, you also have the right to file a police report and get a copy of it.

New York Office of the Attorney General
The Capitol
Albany NY 12224-0341
800.771.7755
www.ag.ny.gov
Note: New York residents may also contact the State for additional information.

New York Department of State
Division of Consumer Protection
99 Washington Avenue, Suite 650
Albany, NY 12231
800.697.1220
www.dos.ny.gov

Oregon Office of the Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
877.877.9392
www.doj.state.or.us