



STATE BREACH NOTIFICATION

February 27, 2023

Anthony G. Brown
Maryland Attorney General
Saint Paul Plaza
200 St. Paul Place
Baltimore, MD 21202

In accordance with Md. Code Com. Law § 14-3501 et seq. of the Maryland state security breach law, I am writing on behalf of Bank of America to inform you of the following incident:

An incident occurred between August 31, 2022, and December 7, 2022, that may have resulted in the disclosure of one client's information by a former employee.

The client will be notified in a letter dated March 6, 2023, with an offer for two years of free credit monitoring.

Pursuant to Md. Code Com. Law § 14-3501 et seq., our compliance with the Interagency Guidance Response Program deems us to be in compliance with the Maryland State Security Breach Law.

The letter addressed to the client is enclosed.

Bennie Barker
Vice President, Sr. Data Architect
Bennie.barker@bofa.com



NOTICE OF DATA BREACH

DATE

Customer Name
Street Address
City, State Zip

Reference Number 2023-677

Customer first and last name:

WHAT HAPPENED: An incident occurred between August 31, 2022, and December 7, 2022, that resulted in the disclosure of your information by a former employee.

WHAT INFORMATION WAS INVOLVED: According to our records, the information involved in this incident was related to your deposit account/debit card and may have included your first and last name, address, property address, email address, phone number, age, gender, date of birth, driver's license number, passport number, Social Security number, user code and PIN, debit/credit card number, account number, account balance, account status, CV2 number, and expiration date.

WHAT WE ARE DOING: Keeping your information secure and confidential is one of our most important responsibilities. We sincerely apologize for this incident and regret any concern or inconvenience it may cause you. We are notifying you so we can work together to protect your personal and account information.

Please be advised we have taken the following precautions to protect your personal and account information:

- We plan on working with law enforcement authorities and have conducted our own internal investigation to protect and minimize any financial impact to you.
- We are monitoring your banking relationship and will notify you if we detect any suspicious or unauthorized activity related to this incident.
- We will work with you to resolve unauthorized transactions on your Bank of America accounts related to this incident if reported in a timely manner.
- As an additional measure of protection, Bank of America has arranged for a **complimentary** two-year membership in an identity theft protection service provided by Experian IdentityWorksSM. **You will not be billed for this service.** This product provides you with identity detection which includes daily monitoring of your credit reports from the three national credit reporting companies (Experian, Equifax[®] and TransUnion[®]), internet surveillance, and resolution of identity theft. **This service will expire at the conclusion of the complimentary period and will not automatically renew.** Any renewal of service elected by the customer is paid for by the customer and done directly through Experian IdentityWorksSM. Bank of America has no involvement with respect to any offers, products or services from or through Experian IdentityWorksSM that the customer may choose to enroll in beyond the complimentary membership. To learn more about the complimentary membership and enroll, go to

<https://www.experianidworks.com/bac/> enter your activation code and complete the secure online form. You will need to **enter the activation code provided below to complete enrollment**. If you prefer to enroll by phone, please call Experian IdentityWorksSM at 866.617.1920.

Experian IdentityWorksSM **Web Site:** <https://www.experianidworks.com/bac/>

Your Activation Code: Activation Code

You Must Enroll By: Expiration Date

Engagement number:

WHAT YOU CAN DO: Please be advised we recommend you take the following precautions to protect your personal and account information:

- Please promptly review your credit reports and account statements over the next 12 to 24 months and notify us of any unauthorized transactions or incidents of suspected identity theft related to your Bank of America accounts (refer to tips on back of this letter).
- Enroll in the Credit Monitoring Service offered above.
- Refer to the enclosed "Important tips on how to protect personal information" for additional precautions you can take.

FOR MORE INFORMATION: Should you have any questions regarding this incident or your accounts, please contact Bank of America's Privacy Response Unit toll-free at **1.800.252.2867**. We are here to help and assist you during this process.

We sincerely apologize for this incident and regret any concern or inconvenience it may cause you.

Sincerely,

Privacy Response Unit (PRU)

ENC: Important tips on how to protect personal information

Important tips on how to protect personal information

We recommend that you take the following precautions to guard against the disclosure and unauthorized use of your account and personal information:

- Review your account statements thoroughly and report any suspicious activity to us.
- Report lost or stolen checks, credit or debit cards immediately. Keep a list of your account numbers along with your financial institution's contact information in a separate, secure location.
- Never provide personal information over the phone or online unless you have initiated the call and know with whom you are speaking.
- Do not include your driver's license or Social Security number on checks, preprinted or otherwise.
- Safeguard ATM, credit and debit cards. Memorize PINs (personal identification numbers) and refrain from writing PINs, Social Security numbers or account numbers where they could be found.
- Store checks and account statements in a safe place.
- Reduce the amount of paper you receive containing personal information. Sign up for online statements, direct deposit and pay bills online.
- Destroy or shred any pre-approved credit offers to which you do not respond.
- As a general best practice, we recommend that you change (and regularly update) existing passwords and PIN numbers and monitor all your account(s) including any additional account(s) you may have with other financial institutions to prevent or detect the occurrence of any unauthorized/fraudulent activity.
- Review your credit report at least once every year. Make sure all information is up to date and accurate. If there are any fraudulent transactions, report them immediately and ensure once resolved, the information is deleted from your credit report. In order to report fraudulent transactions, please reference the 'Reporting Fraud' section below. For a free copy of your credit bureau report, contact www.annualcreditreport.com or call toll-free at 1.877.322.8228.
- Beware of common phishing attempts such as mail, phone calls, and emails containing typos or other errors that ask 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. Financial institution emails do not ask for an email reply containing your personal information, such as Social Security number and ATM or Debit Card PIN.
- Install virus and spyware detection software on your computer and update them regularly.
- Download mobile apps from the appropriate vendor. Ensure you update mobile banking apps as new versions become available.
- Limit the information you share on social networking sites such as your full name along with your address, date of birth, and other identifiable information.
- Place a security freeze on your credit reports, free of charge, with each of the three major consumer reporting agencies. Refer to the information below regarding how to place a security freeze and what information you will need to provide to the agencies.

For more information about guarding your account and personal information, as well as our online practices, please visit our Web site www.bankofamerica.com/privacy.

Requesting and placing a security freeze on your credit reports

A security freeze prohibits a credit reporting agency from releasing information from your credit report without your written permission. Please be aware 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 to place, lift, or remove a security freeze. To place a security freeze on your credit reports, send a written request by mail to each consumer reporting agency at the addresses below, or place a security freeze online or over the phone, using the contact information below.

Information needed to place a security freeze

To request a security freeze, you will need to provide some or all of the following information to each credit reporting agency: full name; Social Security number; date of birth; addresses where you lived over the past five years; proof of current address; a legible photocopy of a government issued ID card or driver's license; Social Security Card, pay stub, or W2; and if you are a victim of identity theft, a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Confirmation of security freeze and PIN/password

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

How to lift a security freeze

To lift the security freeze to allow a specific entity or individual access to your credit report, 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, as well as the identities of the entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual. The credit bureaus have between 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 between 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 have been a victim of identity theft or fraud, contact one of the three major credit bureaus to place a fraud alert on your account. A fraud alert will prevent new credit accounts from being opened without your permission.

Equifax	Experian	TransUnion
1.800.525.6285	1.888.397.3742	1.800.680.7289
P.O. Box 105069	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.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 ID Theft Web site at <http://www.consumer.gov/idtheft/> or call **1.877.438.4338**.

Your Bank of America accounts

Report fraudulent activity on your Bank of America accounts or within Online Banking: **1.800.432.1000**.

Iowa residents:

Iowa residents may also wish to contact the Office of the Attorney General on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Massachusetts residents:

Under Massachusetts law, you have the right to obtain any police report if one was filed. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Maryland residents:

Maryland residents may wish to review the information with the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us.

North Carolina residents:

You can also contact the state of North Carolina's Attorney General at 919.716.6000 or www.ncdoj.gov

Oregon residents:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us.

Rhode Island residents:

Rhode Island residents have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov.