



STATE BREACH NOTIFICATION

January 23, 2023

Attorney General
Maryland
idtheft@oag.state.md.us

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 January 15, 2021, through October 25, 2022, that resulted in the disclosure of client information by a former employee for the purpose of engaging in fraud.

The incident resulted in the disclosure of 4 Maryland residents' information. The information exposed as a result of this incident included: first and last name, address, phone number, email address, age, DOB, gender, driver's license number, Social Security number, user code/PIN, account number, debit/credit card number, account balance/status, CV2, expiration date and routing number. We are aware of resulting fraud to consumers.

The 4 Maryland residents will be notified of this incident in a letter dated 02/01/2023 which included an offer for two years' 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 clients is enclosed.

Bennie L Barker III
Vice President -Privacy Operations
100 N Tryon St. Charlotte, NC
PH: 980-301-3647



NOTICE OF DATA BREACH

DATE

Customer Name
Street Address
City, State Zip

Reference Number 2023-84

Customer first and last name:

WHAT HAPPENED: An incident occurred between January 15, 2021 through October 25, 2022, that resulted in the disclosure of your information by a former employee for the purpose of engaging in fraud. We believe that this incident is related to your previous fraud claim.

WHAT INFORMATION WAS INVOLVED: According to our records, the information involved in this incident was related to your deposit account(s) and may have included your first and last name, address, phone number, email address, age, DOB, gender, driver's license number, Social Security number, user code/PIN, account number, debit/credit card number, account balance/status, CV2, expiration date and routing number. In addition, the deceased joint account holder was also impacted, and the information above would apply for the deceased individual as well.

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 in addition to the decedent's personal and account information.

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

- We 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.
- Please refer to the enclosure for additional precautions you can take to protect the decedent's personal and account information.

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

ENC: Protecting Deceased Individuals

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 number 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 number 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
1.800.525.6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
1.888.397.3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
1.800.680.7289
P.O. Box 6790
Fullerton, CA 92834-6790
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 filed in regard to this incident. In this instance, no police report has been 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.

Protecting Deceased Individuals

Experian has collaborated with the Identity Theft Resource Center (ITRC) to provide information on steps you can take when a deceased or incapacitated loved one is affected by a data compromise incident.

Deceased

Decrease the risk of their identity theft regardless of age by following these steps:

- 1) Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
- 2) If there is a surviving spouse or other joint account holders, make sure to immediately notify relevant credit card companies, banks, stock brokers, loan/lien holders, and mortgage companies of the death. They may require a copy of the death certificate to do this, as well as permission from the survivor, or other authorized account holders.
- 3) The executor or surviving spouse will need to discuss all outstanding debts and how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask them to list it as: "Closed. Account holder is deceased."
- 4) Contact all CRAs (**see contact information below**), credit issuers, collection agencies, and any other financial institution that need to know of the death using the required procedures for each one. The following are general tips:
 - a. Include the following information in all letters:
 - i. Name and SSN of deceased
 - ii. Last known address
 - iii. Last 5 years of addresses
 - iv. Date of birth
 - v. Date of death
 - vi. To speed up processing, include all requested documentation specific to that agency in the first letter
 - b. Send the appropriate Court signed Executive papers
 - c. Send all mail certified, return receipt requested.
 - d. Keep copies of all correspondence, noting date sent and any response(s) you receive.
 - e. Request a copy of the decedent's credit report – See sample template below. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc) so that you can follow through with those entities.
 - f. Request that the report is flagged with the following alert: "Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Note: Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on

a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by-case basis. You may also apply to the courts to be named as an executor of the estate.

Other groups to notify:

- Social Security Administration
- Insurance companies – auto, health, life, etc.
- Veteran's Administration - if the person was a former member of the military
- Immigration Services - if the decedent is not a U.S. citizen
- Department of Motor Vehicles if the person had a driver's license or state ID card. Also make sure that any vehicle registration papers are transferred to the new owners
- Agencies that may be involved due to professional licenses – bar association, medical licenses, cosmetician, etc.
- Any membership programs- video rental, public library, fitness club, etc.

Specific Credit Reporting Agencies (CRAs) information for ordering a credit report or place a deceased flag:

Experian P.O. Box 9701 Allen, TX 75013	
<u>To order a credit report:</u> A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone and Internet. The spouse is legally entitled to the report. The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.	<u>For requests or changes:</u> A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request. After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor. If identity theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased. If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."
Equifax Information Services LLC Office of Consumer Affairs	

P.O. Box 105139,
Atlanta, GA 30348

To Order a credit report:

Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's file. The request should include the following:

A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)

For requests or changes:

Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above.

Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.

TransUnion
P.O. Box 6790
Fullerton, CA 92834

To Order a credit report:

TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file.

If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TransUnion will mail a credit file to the surviving spouse.

If the deceased is a minor child of the requestor, TransUnion will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.

For requests or changes:

Placing a "decease alert" on reports: TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so. The requestor's phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TransUnion will entirely suppress the decedent's credit file and so note it as a deceased consumer. TransUnion will not mail out a copy of its contents without the requirements mentioned above.

If you suspect fraud, TransUnion suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com.

Legal Notice

The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Sample Template

Credit Report Request for the Deceased

Sent credit report request via (include all that apply):

☐ e-mail ☐ fax ☐ mail (certified return receipt requested no.) _____

To (Name of Company): _____

Address: _____

Other Contact Info: _____

Date of Request: _____

Your name: _____

Address: _____

Phone Number (daytime/evening/cell): _____

As the _____ (relationship to deceased), I am notifying you that the following person died.

- Name of deceased: _____
- Date of death: _____
- Date of birth: _____
- Location of birth: _____
- Social Security number of deceased: _____
- Five year address history (most current one first): _____

I would like to make the following requests:

____ I request a current copy of (name of deceased)'s credit report be mailed to me at my address listed above.

____ I request that the following notice be placed on (name of deceased)'s credit report:

"Deceased - Do not issue credit."

____ I request that the following notice also be added to this alert: "If an application is made for credit, notify the following person(s) immediately: _____

____ (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Signed: