Notice of Data Breach

CUSTOMER NAME
ADDRESS
CITY, STATE, ZIP

Reference Number 2026-2628

May 1, 2026

Dear Customer,

WHAT HAPPENED: An incident occurred on or about April 7, 2026, that may have resulted in the disclosure of your information due to your documentation being damaged in transit. We have confirmed that the documents have been returned to the bank.

WHAT INFORMATION WAS INVOLVED: According to our records, the information involved in this incident was related to your trust tax returns and included your first and last name, address, Social Security number, and account number. In addition, for the decedent, Mary Mitchell, her first and last name, address, and Social Security number were impacted.

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, as well as the decedent's 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 unauthorized transactions on your accounts related to this incident if reported in a timely manner.
- We have also arranged for a **complimentary two-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 then complete the secure online form. To enroll by phone, please call Experian IdentityWorks at [TFN).

    Activation code:
    Engagement number:

    You must enroll by October 23, 2026, 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.

Please refer to the *Protecting Deceased Individuals* document we have included for additional information and precautions you can take.

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.
- **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 or concerns, please reach out to me or anyone on your team.

Sincerely,

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.
- 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	**Experian**	**Equifax**
PO Box 2000	PO Box 9554	PO Box 740256
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30374
800.680.7289	888.397.3742	800.525.6285
transunion.com	experian.com	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

Protecting Deceased Individuals

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

Decrease the risk of their identity theft, regardless of age, by doing the following:

- Get at least 12 copies of the official death certificate when it becomes available. In some cases, you'll be able to use a photocopy, but some businesses will require an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
- Make sure, if there's a surviving spouse or other joint account holder(s), to immediately notify relevant credit card companies, banks, stockbrokers, loan or lien holders, and mortgage companies of the death. They may require a copy of the death certificate, as well as permission from the survivor, or other authorized account holder(s).
- Ensure the executor or surviving spouse knows about all outstanding debts and understands how they'll be dealt with. You'll 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."
- Contact all credit reporting agencies (CRAs) listed below, credit issuers, collection agencies, and any other financial institution that needs to know of the death using the required procedures for each one.

Here are general tips:

- Include the following information in all letters:
    - Name and Social Security number (SSN) of the deceased
    - Last known address
    - Last five years of addresses
    - Date of birth
    - Date of death
- To speed up processing, include all requested documentation specific to that agency in the first letter
    - Send the appropriate court signed executive papers
    - Send all mail certified with a return receipt requested.
    - Keep copies of all correspondence, noting the date sent and any response(s) you receive.
    - Request a copy of the decedent's credit report using the sample template we've included.
        - 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 you can follow through with those entities.
- Request the report to be 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)."

Keep in mind, friends, neighbors or distant relatives don't have the same rights as a spouse or executor of the estate. They're 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 unique situation, you can write to the CRA and explain the situation. They're handled on a case-by-case basis. You can 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 wasn't a U.S. citizen
- Department of Motor Vehicles — if the person had a driver's license or state identification (ID) card. Also make sure 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 placing a deceased flag:

Experian
PO Box 4500
Allen, TX 75013

Order a credit report	For change requests
A spouse can get a credit report by making the request through the regular channels — mail, phone and/or Internet. The spouse is legally entitled to the report. The executor of the estate can get a credit report, but must write Experian with a specific request, include a copy of the executor paperwork and the death certificate.	A spouse or executor can request a change to the file to show the person as deceased through a 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 the executor(s) and spouse can request other types of changes that Experian 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 or executor(s) and they must state specifically what they want the general statement to say, such as "Do not issue credit."

Equifax
Office of Consumer Affairs
PO Box 105139
Atlanta, GA 30348-5139

Order a credit report	For change requests
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 a copy of a notarized document stating the requestor is authorized to handle the deceased consumer's affairs (for example: Order from a Probate Court or Letter of Testamentary).	Equifax requests that a spouse, attorney or executor of the estate submit a written request if they want to place a deceased indicator on the deceased consumer's file. The request should be mailed to the above address and include a copy of the consumer's death certificate. Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the file. In addition, Equifax will place a seven-year promotional block on the file. Once Equifax's research is complete, they'll send a response back to the spouse, attorney, or executor of the estate.

Transunion
PO Box 1000
Chester PA, 19016

Order a credit report	For change requests
TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to get a copy of the decedent's credit file. If the requestor is the spouse of the deceased and the address for which the credit file is being mailed to is	TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who identifies themselves as having a right to do so. The requestor's phone number is added to the temporary, three-month alert. Once TransUnion receives a verifiable death

included 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.	certificate, they'll suppress the decedent's credit file and list it as a deceased consumer. TransUnion will not mail out a copy of its contents without these requirements. If you suspect fraud, TransUnion suggests you call their fraud unit at 800.680.7289 or email them at fvad@transunion.com. They'll place a temporary alert over the phone and advise you of what needs to be sent to suppress the credit file and to disclose a copy of its contents.