WILMERHALE

March 24, 2023

Jason C. Chipman

+1 202 663 6195 (t)
+1 202 663 6363 (f)
jason.chipman@wilmerhale.com

VIA EMAIL
Attorney General Brenna Bird
Consumer Protection Division
Office of the Attorney General of Iowa
Hoover State Office Bldg.
1305 E. Walnut Street
Des Moines, IA 50319

Re: *State Breach Notification*

Dear Attorney General Bird:

In accordance with Iowa Code § 715C.1-2 of the Iowa state security breach law, I am writing on behalf of my client Bank of America, N.A. ("Bank of America") to inform you of a security incident at NCB Management Services, Inc. ("NCB") that impacted Bank of America customer information. NCB is a national accounts receivable management company, located at 1 Allied Drive, Trevose, PA 19053-6945, that provides account services to companies, including Bank of America.

NCB discovered on February 4, 2023, that an unauthorized party gained access to NCB's systems on February 1, 2023. It was confirmed on March 8, 2023, that client information previously connected with a Bank of America credit card account was potentially obtained by the unauthorized party. The unauthorized activity on NCB's systems has been stopped, and NCB has obtained assurances that the third party no longer has any of the information on its systems. NCB has also notified law enforcement. We are not aware of any use or distribution of the potentially accessed information. Bank of America's systems were not impacted by this event.

The information involved in this NCB incident may have included details about a credit card account that 1,918 Iowa residents formerly had with Bank of America. This impacted credit card account had already been closed prior to the security incident. The information involved may have included first and last name, address, phone number, email address, date of birth, employment position, pay amount, driver's license number, Social Security number, account number, credit card number, routing number, account balance, and/or account status. Again, we are not aware of any use or distribution of the potentially accessed information.

NCB will begin notifying impacted Bank of America customers beginning March 24, 2023. Bank of America is making available a complimentary two-year membership in an identity theft

protection service for eligible affected customers. Information about these services is contained in the notification letters to the potentially affected customers.

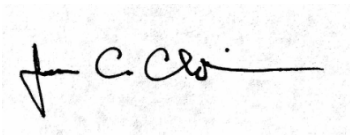
A copy of a model notification letter addressed to the customers is enclosed.

***

Bank of America does not intend to, and does not, waive any applicable privilege. If it were found that any of the information provided constitutes disclosure of otherwise privileged matters such disclosure would be inadvertent.

Please do not hesitate to contact me if you have any questions.

Best regards,



Jason C. Chipman

Enclosure

Attachment
FORM OF INDIVIDUAL NOTICE LETTER

Return Mail Processing
P.O. Box 32624
Charlotte, NC 28232

March 24, 2023

Reference Number [redacted]

FRST_NM LST_NM
ADDR_LIN_1_TX
ADDR_LIN_2_TX
CTY_NM ST_CD ZIP_FRST_5_CD

Re: Notice of Data Breach

Dear [FRST_NM LST_NM]:

We are writing to you in regard to a security incident at NCB Management Services, Inc. ("NCB"). NCB is a national accounts receivable management company that provides account services to companies.

Recently, confidential client account information maintained by NCB was accessed by an unauthorized party. The information involved may have included details about a credit card account that you formerly had with Bank of America. To date, we are not aware of any misuse of your information as a result of this incident. However, in support of you and your information security, we are notifying you and providing tools you can use to protect against possible identity theft or fraud.

WHAT HAPPENED: NCB discovered on February 4 that an unauthorized party gained access to NCB's systems on February 1, 2023. It was confirmed on March 8 that some of your client information previously connected with your Bank of America credit card account was potentially obtained by the unauthorized party. The unauthorized activity on NCB's systems has been stopped, and NCB has obtained assurances that the third party no longer has any of the information on its systems. Bank of America's systems were not impacted by this event.

WHAT INFORMATION WAS INVOLVED: According to our records, the information potentially accessed in this NCB incident was related to a credit card account. This impacted credit card account had already been closed. The information involved may have included your first and last name, address, phone number, email address, date of birth, employment position, pay amount, driver's license number, Social Security number, account number, credit card number, routing number, account balance, and/or account status. We are not aware of any use or distribution of the potentially accessed information.

WHAT WE ARE DOING: We are notifying you so you can protect your personal and account information.

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

- NCB is working with federal law enforcement authorities.
- As an additional measure of protection, we are notifying you that Bank of America will be making available a **complimentary** two-year membership in an identity theft protection service provided by Experian IdentityWorks℠. **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 you and paid by you should be done directly through Experian IdentityWorks℠. To learn more about the complimentary membership and enroll, go to https://www.experianidworks.com/3bcredit 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 IdentityWorks℠ at 800.910.5024.

Experian IdentityWorks℠ **Web Site:** https://www.experianidworks.com/3bcredit
Your Activation Code: **Activation_Code**
You Must Enroll By: **Enrollment End Date**
Engagement number: Experian_Engagement_Number

WHAT YOU CAN DO: We recommend you take the following precautions to protect your personal information:

- Please promptly review your credit reports and account statements over the next 12 to 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft. (Refer to tips on back of this letter).
- Enroll in the complimentary 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: NCB is no longer servicing your closed credit card account with Bank of America. Should you have any questions regarding this incident, please contact Bank of America at [redacted], Monday – Friday between 8am – 11pm ET and Saturday 8am – 8pm ET who can assist you during this process.

We regret any concern or inconvenience this incident at NCB may cause you.

Sincerely,

NCB Management Services, Inc.
1 Allied Drive, Trevose, PA 19053-6945

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 your financial institution.
- 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 any 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. You may also purchase a copy of your credit report by contacting one more of the three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com

- 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.

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**. TTY: (866) 653 – 4261. The FTC's address is: **600 Pennsylvania Avenue, NW, Washington, DC 20580.**

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

District of Columbia residents:
District of Columbia residents may contact their state Attorney General for additional information about avoiding identity theft at 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.

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.

New Mexico residents:
You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

New York residents:
New York residents may contact the New York Attorney General or the New York Department of State for additional information about avoiding identity theft at:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

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.