

February 1, 2024

Jason C. Chipman

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

**CONFIDENTIAL MATERIAL – NOT SUBJECT TO
PUBLIC RECORDS REQUEST**

VIA E-MAIL

Attorney General Anthony G. Brown
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: *State Breach Notification*

Dear Attorney General Brown:

In accordance with MD Commercial Code §14-3504, I am writing on behalf of my client Bank of America, N.A. (“Bank of America”) to inform you of a security incident involving a third-party vendor, Infosys McCamish Systems LLC (“IMS”), that may have impacted some Bank of America employee information and Bank of America clients and the personal information of their plan participants and beneficiaries. IMS provides information technology services to support life insurance, annuity products and deferred compensation plans to companies like Bank of America.

On or around November 3, 2023, IMS disclosed a cybersecurity event resulting in non-availability of certain applications and systems in IMS, including those used by Bank of America. On November 24, 2023, IMS informed Bank of America that Bank of America corporate client data, related to deferred compensation plans managed by Bank of America, may have been compromised as a result of the incident. IMS has informed Bank of America that their investigation will likely never be determinative regarding what personal information was exfiltrated. Out of an abundance of caution, we are reporting this incident on behalf of Bank of America, and on behalf of Bank of America’s clients. Bank of America’s systems were not impacted by this event.

The information involved in this incident may have included details about the financial account information of seven hundred eighty-three (783) Maryland residents. Particularly, the information involved may have included first and last name, address, email address, date of birth, Social Security number, or other forms of identification and/or financial account information.

Page 2

Bank of America will begin notifying potentially impacted individuals via U.S. Mail beginning February 1, 2024. Additionally, Bank of America is making available a complimentary two-year membership in an identity theft protection service for eligible affected individuals. Information about these services is contained in the notification letters to the potentially affected individuals.

A copy of a model notification letter addressed to participants is enclosed as **Attachment A**.

Bank of America respectfully requests that your office contact WilmerHale in the first instance should you have any questions or follow-up from this notification letter. We are also providing the following contact information for the entity that experienced the breach, IMS:

Ron Plesco (Outside Counsel for IMS)
Email: ron.plesco@dlapiper.com
Telephone: +1 215 656 2453

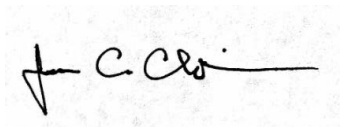
WilmerHale has designated this letter as confidential because it contains confidential and proprietary business information that is exempt from a public information request. See Md. Code § 4-335. We request that you take all available steps to prevent the disclosure of this letter to third parties.

We assert all available protections regarding this information so that it will not be released without Bank of America's written authorization.

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,

A handwritten signature in black ink, appearing to read "J. C. Chipman", written over a light blue textured background.

Jason C. Chipman

Enclosure

Attachment A
FORM OF INDIVIDUAL LETTER

[DATE]

[Customer Name
Street Address
City, State Zip]

Re: Notice of Data Breach

Dear [Participant first and last name]:

We are writing to you about a security incident at Infosys McCamish Systems LLC (“IMS”). IMS provides services for deferred compensation plans, including plans serviced by Bank of America that you were eligible to participate in. Out of an abundance of caution, we are notifying you about this incident and providing tools to help you protect against possible identity theft or fraud.

What Happened: On or around November 3, 2023, IMS was impacted by a cybersecurity event when an unauthorized third party accessed IMS systems, resulting in the non-availability of certain IMS applications. On November 24, 2023, IMS told Bank of America that data concerning deferred compensation plans serviced by Bank of America may have been compromised. Bank of America’s systems were not compromised.

In response to the security incident, IMS retained a third-party forensic firm to investigate and assist with IMS’s recovery plan, which included containing and remediating malicious activity, rebuilding systems, and enhancing response capabilities. To date, IMS has found no evidence of continued threat actor access, tooling, or persistence in the IMS environment.

What Information Was Involved: It is unlikely that we will be able to determine with certainty what personal information was accessed as a result of this incident at IMS. According to our records, deferred compensation plan information may have included your first and last name, address, business email address, date of birth, Social Security number, and other account information.

What We Are Doing: Although we are not aware of any misuse involving your information, we are notifying you that Bank of America will provide a **complimentary** two-year membership in an identity theft protection service provided by Experian IdentityWorksSM. **You will not be billed for this service, but you must enroll for activation.** This product provides you with 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 IdentityWorksSM. To enroll, go to <https://www.experianidworks.com/bac/> or call Experian IdentityWorksSM at [enter TFN]. You will need **the activation code and engagement number provided below to complete enrollment.**

Your Activation Code: [Activation Code]

You Must Enroll By: [Expiration Date]

Engagement number: [Engagement Number]

What You Can Do: We recommend you take the following steps to help protect your personal information:

- Promptly review your credit reports and account statements over the next 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft.
- Enroll in the complimentary identity theft protection service offered above.

We also recommend that you review the additional information about ways to protect your identity or any additional rights you have depending on your jurisdiction, both provided in **Attachment A**.

For More Information: Should you have any questions regarding this incident, please contact Bank of America at [enter TFN], Monday – Friday between 8am – 9pm ET, excluding major U.S. holidays.

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

Sincerely,

Infosys McCamish Systems LLC

ENC: Attachment A: Additional Information on Protecting Your Information and State Law Information

Attachment A: Additional Information on Protecting Your Information and State Law Information

Monitor Your Accounts

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies identified above.

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze: Full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past five (5) years; proof of current address, such as a current utility bill or telephone bill; and other personal information as required by the applicable credit reporting agency. If you request a credit freeze online or by phone, the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file. If you request a lift of the credit freeze online or by phone, the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, the credit reporting agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert lasts 1-year. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which lasts 7 years. Should you wish to place a fraud alert, please contact any one of the major consumer reporting agencies listed above. The agency you contact will then contact the other two credit agencies.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. **The Federal Trade Commission:** 600 Pennsylvania Avenue, NW Washington, DC 20580. 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261; and www.ftc.gov/idtheft.

For residents of the District of Columbia, Iowa, Maryland, New York, North Carolina, Oregon and Rhode Island

You may contact your Attorney General for additional information about avoiding identity theft. If you are a Rhode Island resident, you may also file a police report by contacting local or state law enforcement agencies. You may use the following information to contact your attorney general:

Office of the Attorney General Office of Consumer Protection 400 6th Street, NW Washington, DC 20001 (202) 442-9828 www.oag.dc.gov	Office of the Iowa Attorney General Hoover State Office Building 1305 E. Walnut Street Des Moines, IA 50319 (515) 281-5926 / (888) 777-4590 www.iowaattorneygeneral.gov	Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (410) 528-8662 www.marylandattorneygeneral.gov	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (877) 877-9392 www.doj.state.or.us
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, New York 12231 (800) 697-1220 www.dos.ny.gov	North Carolina Department of Justice 9001 Mail Service Center Raleigh, NC 27699-9001 (919) 716-6000 www.ncdoj.gov	Rhode Island Office of the Attorney General Consumer Protection Division 150 South Main Street Providence, RI 02903 (401) 274-4400 www.riag.ri.gov

For residents of Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: 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.