

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

November 17, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: New York City Bar Association – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents the New York City Bar Association (“NYC Bar”) of New York City, New York. I am writing to provide notification of an incident that may affect the security of personal information of approximately sixty-three (63) Maryland residents. By providing this notice, NYC Bar does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about December 24, 2022, NYC Bar experienced a cybersecurity incident that impacted connectivity to its network. Upon experiencing the incident, NYC Bar’s internal IT specialists took its networks offline to contain the threat and immediately commenced a prompt and thorough investigation with external forensic investigators and data privacy professionals.

After an extensive forensic investigation and manual document review, NYC Bar discovered on October 18, 2023 that between December 2, 2022 and December 24, 2022, certain impacted files may have been removed from the NYC Bar by an unauthorized individual contained personal information pertaining to a limited number of Maryland residents, such as account number, routing number, driver’s license or state ID, medical information, health insurance information, payment card number Social Security number, passport number, U.S. Alien registration number and biometric data.

NYC Bar is providing the affected residents with written notification of this incident commencing on or about November 17, 2023 in substantially the same form as the letter attached hereto. NYC Bar will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General. Further, complimentary credit monitoring services were provided for those with impacted Social Security numbers.

At NYC Bar, protecting the privacy of personal information is a top priority. NYC Bar is committed to maintaining the privacy of personal and financial information in its possession and has taken many precautions to safeguard it.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,



Nicholas A. Kurk

Encl.

NEW YORK
CITY BAR

P.O. Box 989728
West Sacramento, CA 95798-9728

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

[REDACTED]

[REDACTED]

November 17, 2023

Dear [REDACTED]

We are writing to inform you of a data security incident at the New York City Bar Association (“NYC Bar”) involving some of your information. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about December 24, 2022, NYC Bar experienced a cybersecurity incident that impacted connectivity to our network.

What We Are Doing.

Upon experiencing the incident, NYC Bar’s internal IT specialists took our networks offline to contain the threat and immediately commenced a prompt and thorough investigation. As part of our investigation, NYC Bar has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, NYC Bar discovered on October 18, 2023 that between December 2, 2022 and December 24, 2022, certain impacted files may have been removed from the NYC Bar by an unauthorized individual.

What Information Was Involved?

The information potentially impacted by the unauthorized party included your name and [REDACTED]
[REDACTED]

What You Can Do.

While we have no evidence of financial fraud or identity theft related to this data, we want to make you aware of the incident. To protect you and your information, we are providing you with [REDACTED] months of free credit monitoring and identity theft protection services through IDX, a Zero Fox Company. This service provides credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information, contact IDX with any questions and to enroll in free identity protection services call [REDACTED], go to [REDACTED], or scan the QR image and use the Enrollment Code provided above. IDX representatives are available [REDACTED]
[REDACTED]. Please note the deadline to enroll is [REDACTED].

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

New York City Bar Association

42 W. 44TH St.

New York, NY 10036

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Months Credit Monitoring

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary [REDACTED]-month credit monitoring services, we recommend that you place an initial one (1) year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069

Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department

P.O. Box 2000

Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at

www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

February 23, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: New York City Bar Association – Supplemental Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents New York City Bar Association (“NYC Bar”). In response to a small portion of undeliverable letters, NYC Bar identified additional Maryland residents impacted by the incident for which we first notified your office on November 17, 2023. Around the time of the initial mailing, NYC Bar effectuated notice both through direct mail and complying with New York's substitute notification provisions. Nonetheless, after discovering that a subset of letters were not delivered, NYC Bar conducted an extensive address search and remailed letters to twelve (12) Maryland residents on February 21, 2024. After the address search, the total number of impacted Maryland residents is seventy-three (73). There were no additional impacted individuals and the change in impacted individuals is due solely to the additional address search. By providing this notice, NYC Bar does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,



Nicholas A. Kurk

Encl.