

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

June 29, 2023

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

Brian E. Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: KBF CPAs – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents KBF CPAs (“KBF”). I am writing to provide notification of an incident at KBF that may affect the security of personal information of three (3) Maryland residents. KBF’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, KBF does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

In November 2022, an unauthorized individual obtained access to a third-party storage platform used by KBF. Upon learning of the issue, KBF immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. KBF devoted considerable time and effort to determine what information was contained in the impacted documents. Based on this comprehensive investigation and manual document review, KBF determined on June 6, 2023 that the impacted documents contained a limited amount of personal information, including the affected residents’ full names, Social Security numbers, driver’s license numbers, and financial account information.

KBF has no indication that any information has been misused. Nevertheless, out of an abundance of caution, KBF wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. KBF is providing the affected residents with notification of this incident commencing on or about June 29, 2023 in substantially the same form as the letter attached hereto. KBF is providing the affected residents with 12 months of complimentary credit monitoring services and is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. KBF is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and

June 29, 2023

Page 2

obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At KBF, protecting the privacy of personal information is a top priority. KBF is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. KBF continually evaluates and modifies its practices and internal controls to enhance the security and privacy of the personal information.

Should you have any questions concerning this notification, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Nicholas A. Kurk

Encl.

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to KBF CPAs ("KBF"). As such, we wanted to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that in November 2022, an unauthorized individual obtained access to a third-party storage platform used by KBF.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on June 6, 2023 that a limited number of documents stored by KBF on the third-party storage platform were potentially accessed or acquired by the unauthorized individual.

What Information Was Involved?

The impacted documents contained some of your personal information, specifically your [REDACTED]

What You Can Do.

To protect you from potential misuse of your information, we are providing you with complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company. For more information on identity theft prevention and instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

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. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

If your tax return was rejected **or** you received a tax notice from a government agency (such as a notice from the IRS indicating someone was otherwise using your Social Security number), we recommend that you follow the below guidance:

- Respond immediately to any IRS notice you receive, and call the number provided and/or follow the instructions contained in the notice;
- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/fl4039.pdf>).**
 - ***Additional instructions for filing the Affidavit are included on the following pages.***
- You may choose to opt-in to the IRS Identity Protection (IP) PIN Program. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. To opt-in, you should use the online “Get an IP PIN” tool (which can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>). If you don’t already have an account on IRS.gov, you must register to validate your identity. An IP PIN is valid for one calendar year. You must obtain a new IP PIN each year. The IP PIN tool is generally unavailable mid-November through mid-January each year.
- If you are filing Form 14039, you should also check with your local state tax agency to see if there are any additional steps to take at the state level for reporting tax-related identity theft;
 - A complete listing of each state tax agency’s website can be found at: <https://www.taxadmin.org/state-tax-agencies>. ***Additional information for reporting tax-related identity fraud to state tax agencies can be found on the following pages.***
- Review guidance from the IRS about tax-related identity theft at: <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft> (*Taxpayer Guide to Identity Theft*) and <https://www.irs.gov/pub/irs-pdf7p5027.pdf> (*IRS Publication 5027, Identity Theft Information for Taxpayers*), and/or
- Call or visit your local law enforcement agency and file a police report.

Keep in mind that if you have an open identity theft case that is being worked on by the IRS, you need to continue to file your tax returns while the investigation is ongoing. Additional information regarding preventing tax related identity theft can be found at: <http://www.irs.gov/Identity-Protection>. In addition to the above, we also recommend that you take additional steps with agencies outside of the IRS, and report incidents of identity theft to the Federal Trade Commission and contact the fraud departments of the three major credit bureaus. More information, including contact information, for these agencies can be found in the attachment.

For More Information.

Please accept our apologies that this incident occurred. We remain fully 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 to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at ^^^^^^^^| This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available **H|||||S|||||K** [REDACTED]

Sincerely,

KBF CPAs
5285 Meadows Rd
Lake Oswego, OR 97035

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 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

<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 LLC

Fraud Victim Assistance

Department

P.O. Box 2000

Chester, PA 19016-2000

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. 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 charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<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-f>

(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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

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: 1-888-743-0023.

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 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

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.

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.

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 www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

6. Reporting Identity Fraud to the IRS.

As noted above, if you believe that you are a victim of identity fraud AND it is affecting your federal tax records (*or may affect* them at some time in the future), it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>)**
 - This form gets mailed or faxed to the IRS: Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
 - ***Please note that this form should be used *only* if your Social Security number has been compromised and the IRS has informed you that you may be a victim of tax-related identity fraud or your e-file return was rejected as a duplicate.**
- Call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm ET); and/or
- You may call or visit your local law enforcement agency and file a police report. Please bring this notice with you.

Additional information regarding preventing tax-related identity theft can be found at: <http://www.irs.gov/uac/Identity-Protection>. For further information and guidance from the IRS about tax-related identity theft, please visit: <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft> (Taxpayer Guide to Identity Theft) and <https://www.irs.gov/pub/irs-pdf/p5027.pdf> (IRS Publication 5027, Identity Theft Information for Taxpayers).

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess to block electronic access to your Social Security record. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>. This publication provides additional information on the potential impact of identity theft to your Social Security number and what actions you should take.

8. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.