McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

**Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM**
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

March 23, 2023

**VIA ONLINE PORTAL**

Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

**Re: Abbey Tax, LLC – Incident Notification**

Dear Mr. Frey:

McDonald Hopkins PLC represents the Abbey Tax, LLC ("Abbey Tax") located at P.O. Box 928 Liberty Lake, WA 99019. I am writing to provide notification of an incident at Abbey Tax that may affect the security of personal information of one (1) Maine resident. By providing this notice, Abbey Tax does not waive any rights or defenses regarding the applicability of Maine or personal jurisdiction.

On October 5, 2022, Abbey Tax learned their EFIN was used to file fraudulent tax returns during the 2021 tax year for individuals that were not current or former clients of Abbey Tax. Upon learning of the issue, Abbey Tax commenced an immediate and thorough investigation. As part of its investigation, Abbey Tax engaged leading third-party experts experienced in handling these types of incidents.

The investigation did not identify unauthorized access to any personally identifiable information, however, there was evidence of malware on one of the systems used for the business. The information maintained on the impacted system includes full names, Social Security numbers, and financial account information.

Abbey Tax will be providing the affected resident with written notification of this incident commencing on or about March 23 2023, in substantially the same form as the letter attached hereto.

**Abbey Tax has no evidence of identity theft related to this incident.** However, out of an abundance of caution, Abbey Tax wanted to inform your Office (and the affected resident) of the incident. Notified individuals will be provided with best practices to protect their information, including but not limited to complimentary credit monitoring services.

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

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl.



McDonald Hopkins
A business advisory and advocacy law firm®

Abbey Tax, LLC
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07286 4-1

# ABBEY TAX, LLC

[redacted]

March 23, 2023

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

At Abbey Tax, LLC ("Abbey Tax"), maintaining our client's trust and protecting our client's personal information are among our highest priorities. We are writing with important information regarding a recent potential data security incident which may have impacted current or former clients, their spouses or significant others filing jointly, and their dependents. We want to provide 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 October 5, 2022, Abbey Tax learned that our EFIN was used to file fraudulent tax returns during the 2021 tax year. The individuals identified at that time were not current or former clients of Abbey Tax.

*What We Are Doing.*

Upon learning of the incident, Abbey Tax coordinated with the IRS to provide them with more information, obtained a new EFIN number, and provided specific information to the IRS in order to protect Abbey Tax clients from potential fraudulent returns. Additionally, upon learning of this issue, we immediately commenced a prompt and thorough investigation into our information systems. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents to analyze the extent of any compromise of the information on our network. After an extensive forensic investigation we discovered malware on one of our corporate devices that may have provided access to an unauthorized party. Abbey Tax communicated with the security and privacy professionals to analyze and mitigate any potential issues. Abbey Tax also changed all of its user's login credentials.

*What Information Was Involved?*

While the investigation did not confirm that any of your information was accessed or obtained as a result of the incident, the personal information that we maintain includes your full name and [redacted].

*What You Can Do.*

Out of an abundance of caution, to protect you and your information, we are providing 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 [redacted] 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 specializing in fraud assistance and remediation services.

For more information on identity theft prevention, including instructions on how to activate your complimentary monitoring services membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your information, including placing a fraud alert and/or security freeze on your credit files, obtaining a free credit report, and/or reporting fraudulent activity to the IRS. 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*.

We regret any inconvenience that this may cause you. 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.

If you have any further questions regarding this incident, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. Please call the help line [redacted] and supply the fraud specialist with your unique code listed below.

Sincerely,

Abbey Tax, LLC

**– OTHER IMPORTANT INFORMATION –**

**1. Enrolling in Complimentary [redacted] Month Credit Monitoring.**

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 [redacted] month credit monitoring services, we recommend that you place an initial one-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. 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/
(800) 349-9960
(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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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.

**6. Reporting Identity Fraud to the IRS.**

If your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, 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)**
    - *Instructions for Form 14039* – In Section A check box 1. / In Section B check box 2. / Insert this in the "Please provide an explanation" box: I receive notice that my name and Social Security number may have been used to file a fraudulent tax return that was accepted by the IRS and/or state tax agency.
        - This form should be mailed or faxed to the IRS: Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
- 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); and/or
- File a police report with your local police department. It may be appropriate to provide a copy of this letter.

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).

**You may request an IRS Identity Protection PIN (IP PIN) at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps IRS verify your identity when you file your electronic or paper tax return.**

- **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.