McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P: 1.410.917.5189

**Spencer S. Pollock**
Direct Dial: (410) 917 5189
E-mail: spollock@mcdonaldhopkins.com

January 22, 2025

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

Attorney General Anthony G. Brown
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

**Re: Perkins Law – Incident Notification**

Dear Attorney General Brown:

McDonald Hopkins PLC represents Perkins Law. I am writing to provide notification of an incident at Perkins Law that may affect the security of personal information of approximately one (1) Maryland resident. Perkins Law'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, Perkins Law does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Perkins Law experienced a security incident that impacted their network on or about October 9, 2024. Upon learning of this issue, Perkins Law immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, Perkins Law engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the Perkins Law network. Based on the comprehensive investigation, Perkins Law concluded that certain documents and records maintained within their possession were accessed and/or obtained in connection with this incident. Following the extensive manual document review, Perkins Law determined on January 7, 2025 that certain personal information was present in those documents and records. The impacted data includes full name in combination with Social Security number, date of birth, account number and routing number. On January 14, 2025, Perkins Law located the most recent contact information for the impacted individual.

To date, Perkins Law is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, Perkins Law is providing notice to the affected clients commencing on January 22, 2025 in substantially the same form as the enclosed letter (Attached as Exhibit A). The notified individuals who have had their Social Security number impacted will receive complimentary credit monitoring services. Additionally, Perkins Law will advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Perkins Law will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for Perkins Law. Perkins Law remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Perkins Law continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (410) 917 5189 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Spencer S. Pollock

Encl.

# Exhibit A

Perkins Law LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PERKINS LAW LLC

[redacted]

000010102G0500

P

[redacted]

IMPORTANT INFORMATION, PLEASE REVIEW CAREFULLY

Dear [redacted]:

I am writing with important information regarding a recent data security incident that Perkins Law experienced. The privacy and security of the protected personal information entrusted to us is of the utmost importance to Perkins Law. As such, 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?*

We experienced a security incident on or about October 9, 2024, that impacted our network environment. After a thorough investigation and extensive review of impacted data, we discovered on January 7, 2025, that the files the unauthorized actor downloaded contained some of your personal information. We want to make you aware of the incident and provide you with steps you can take to further protect your information.

*What Are We Doing?*

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and notified the FBI of the incident. Additionally, Perkins Law is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to further mitigate risks of this nature. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your protected personal information.

*What Information Was Involved?*

The data that the unauthorized actor downloaded contained some of your protected personal information, including your [redacted].

*What Can You Do?*

We have no evidence that any of your information has been used for identity theft or to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. 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 from potential misuse of your information, we are offering a complimentary [redacted] month membership of **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. 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 the event you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other precautionary measures 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.*

We sincerely regret the occurrence of this incident. We are committed to maintaining the proper handling, protection, and privacy of protected personal information in our possession and have taken precautions to safeguard it.

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 [redacted] Representatives are available from 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information.

Sincerely,

Perkins Law, LLC
1575 Burns Street
West Linn, OR 97068

## - 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 by April 17th, 2025**. The enrollment requires an internet connection and e-mail account. 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.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 90-day "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 will 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.

0000102028000 P

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 TTY: 1-866-653-4261, 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.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. - 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

**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.

**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.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.