McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

October 27, 2022

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Carolyn Secor, P.A. – Incident Notification

Dear Attorney General Formella:

McDonald Hopkins PLC represents Carolyn Secor, P.A. ("CS"), located at 2451 McMullen Booth Rd Suite 200, Clearwater, FL 33759. I am writing to provide notification of an incident at CS that may affect the security of personal information of one (1) New Hampshire resident. By providing this notice, CS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 2, 2022 an unauthorized party accessed CS's systems. Upon detecting the incident, CS commenced an immediate and thorough investigation. As part of the investigation, CS worked to identify what personal information, if any, might have been present in the accessed systems.

After an extensive investigation and manual document review, CS determined that the systems accessed contained personal information pertaining to a limited number of individuals, such as full names, Social Security number, credit or debit card information, bank account information and routing number, and driver's license or state identification number.

CS provided the affected New Hampshire resident with written notification of this incident commencing on October 27, 2022, in substantially the same form as the letter attached hereto.

CS is not aware of any reports of identity fraud or improper use of personal information as a direct result of this incident. However, out of an abundance of caution, CS wanted to inform your Office (and the affected residents) of the incident. Notified individuals have been provided with best practices to protect their information, including but not limited to complimentary credit monitoring services which were provided to those individuals whose Social Security numbers may have been impacted by this incident.

At CS, protecting the privacy of personal information is a top priority. CS is committed to maintaining the privacy of personal information in its possession and has taken precautions to safeguard it. CS 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 (410) 917-5189 or spollock@mcdonaldhopkins.com.

Very truly yours,

Spencer S. Pollock

Encl.

Carolyn Secor, P.A.
[redacted]

Carolyn Secor, P.A.
2451 N. McMullen Booth Road
Suite 200
Clearwater, FL 33759
(727) 254-1704
www.bankruptcyfortampa.com

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Carolyn Secor, P.A. ("CS"). We are writing with important information regarding a recent data security incident that may have involved some of your information. We want 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?

On July 2, 2022, we detected unauthorized access to our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network and immediately commenced prompt and thorough remediation measures. As part of our remediation efforts, 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. Due to a lack of available evidence, we were unable to rule that certain files containing your personal information were exposed for access or potentially acquired by an unauthorized individual(s). Therefore, we are providing you with the notification out of an abundance of caution.

What Information Was Involved.

The files contained on our system at the time of the unauthorized access may have included all or some of the following personal information: your name, Social Security number, credit or debit card information, bank account information and routing number, and driver's license or state identification number.

What You Can Do.

We have no evidence that any of your information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering access to Single Bureau Credit Monitoring* services at no

* Services marked with an "*" require 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.

charge. These services provide you with alerts for [redacted] 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

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 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 [redacted]. 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 for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday.

Sincerely,

Carolyn Secor, P.A.

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

To enroll in Credit Monitoring* services at no charge, please log on to https://secure.identityforce.com/benefit/cspa 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted] 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	*Experian*	*TransUnion LLC*
P.O. Box 105069 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	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	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (800) 349-9960	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	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 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: 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.