McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

August 15, 2018

Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301

Re: Cain Watters & Associates – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Cain Watters & Associates ("Cain Watters"). I write to provide notification concerning an incident that may affect the security of personal information of one (1) New Hampshire resident. Cain Watters' 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, Cain Watters does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Cain Watters recently discovered on June 28, 2018 that one of its email accounts was compromised by an unauthorized third party. Cain Watters immediately launched an investigation in consultation with outside cybersecurity experts to analyze the extent of any compromise to the email account and the security of the emails and attachments contained within. Cain Watters' investigation determined that there were unauthorized logins to the affected account between May 25, 2018 and June 28, 2018. Cain Watters devoted considerable time and effort to determine what information was contained in the affected email account. Based on the comprehensive investigation and document review, which concluded on July 25, 2018, Cain Watters discovered that the compromised email account contained the financial account number of one (1) New Hampshire resident.

To date, Cain Watters is not aware of any reports of identity fraud or improper use of the resident's information as a direct result of this incident. Cain Watters nevertheless wanted to make you (and the affected resident) aware of the incident out of an abundance of caution and explain the steps Cain Watters is taking to help safeguard the resident against financial fraud. Cain Watters will provide the New Hampshire resident with written notice of this incident commencing on August 16, 2018, in substantially the same form as the letter attached hereto. Cain Watters will provide the affected resident with paperwork to effectuate a change in the potentially exposed account number. Cain Watters will advise the resident to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Cain Watters will also advise the resident about the process for placing a fraud alert on their credit file, placing a

security freeze, and obtaining a free credit report. The resident will additionally be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Cain Watters, protecting the privacy and security of personal information is a top priority. To help prevent a similar incident from occurring in the future, Cain Watters has reset passwords.

Should you have any questions regarding this notification, please contact me at 248.220.1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

Encl.

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

Dear [redacted]

I am writing to provide you with important details about a recent incident involving the security of your information and the measures we are taking to protect your information.

We recently discovered on June 28, 2018 that a Cain Watters & Associates email account was compromised by an unauthorized third party. We immediately launched an investigation in consultation with outside cybersecurity experts to analyze the extent of any compromise to the email account and the security of the emails and attachments contained within. Our investigation determined that there were unauthorized logins to the affected account between May 25, 2018 and June 28, 2018.

We devoted considerable time and effort to determine what information was contained in the affected email account. Based on our comprehensive investigation and document review, which concluded on July 25, 2018, we discovered that the compromised email account contained your full name and financial account number.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. However, out of an abundance of caution, we wanted to make you aware of the incident and suggest steps that you should take as well. Further, you should remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. We are also enclosing paperwork with this letter to effectuate a change in your financial account number. Please complete it and return it to me at your earliest convenience. Additionally, enclosed in this letter, you will find precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report.

We take the security of personal information very seriously, and apologize for any inconvenience this incident may cause you. Among other things, we have reset passwords to prevent further unauthorized access to this information.

If you have any further questions regarding this incident, please call us directly at [redacted]. We are available Monday through Friday, 9:00 a.m. to 5:00 p.m. Central Time.

Sincerely,

[redacted]

Cain Watters & Associates, LLC

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Placing a Fraud Alert

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. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. 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. 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 or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872
1-800-349-9960 (NY residents only)		

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 monitoring 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.

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies' websites to find out the specific costs applicable to the State in which you currently reside.

If you decide to place a Security Freeze on your credit file, *in order to do so without paying a fee*, you will need to send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services. 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.

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. After you sign up for the credit monitoring service, you may refreeze your credit file. We encourage you to wait to place a security freeze on your credit file until you have enrolled in the credit monitoring service to avoid paying additional fees related to placing an initial security freeze on your credit file, temporarily lifting or removing the security freeze and subsequently refreezing your credit file.

3. 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 that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. 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 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.

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.

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, Department of Justice, 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, and report suspected identity theft to, 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.