

April 11, 2019

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

This notice is provided on behalf of my client Wingate Wealth Advisors (“Wingate”), pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). As a result of its investigation, Wingate determined that some of the personal information that it maintained about some of its clients and their families, as well as other information about Wingate’s business, its employees and related activities may have been accessed without authorization.

On February 1, 2019, Wingate learned that a large number of emails had been sent from the account of one of its employees without authorization. Wingate immediately notified its cybersecurity insurance company and began working with experts to determine what had happened and how. On February 5, 2019, Wingate first learned that there had been incidents of unauthorized access to the affected employee’s email account between January 9, 2019 and February 1, 2019. The Wingate employee had permission to access the email accounts of two other Wingate employees.

During the course of Wingate’s investigation of the first incident, it experienced a second incident that may have involved unauthorized access to two additional Wingate employee email accounts, between February 19, 2019 and February 27, 2019. Wingate conducted a comprehensive review of every email in the email accounts impacted by the first and/or second incidents to determine what specific information was in each email and who may have been affected. As a result of its review, Wingate determined that personal information including first and last name, address, Social Security number, driver’s license, or other government identification was contained in the email accounts, and may have been potentially affected. At this time, Wingate has no indication that information affected by these incidents has been inappropriately used by anyone.

Since Wingate discovered these incidents, it has taken several steps to enhance security and to help prevent something like this from happening again. Specifically, Wingate:

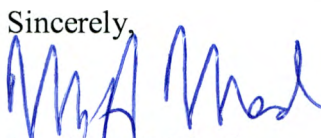
STATE OF NH  
DEPT OF JUSTICE  
2019 APR 16 PM 12:03

1. Reset the passwords of the impacted email accounts.
2. Notified the brokerage custodians which hold most of Wingate's clients' funds of the incidents. These institutions have placed all of Wingate's clients' accounts on a heightened security watch status, and will alert Wingate in the event of any unusual activities in any of its clients' accounts.
3. Confirmed that the brokerage custodians which hold most of Wingate's clients' funds have corporate policies that provide for fraud protection for clients' accounts in the event of any unauthorized activity. It is their policy is to reimburse clients in the event of any unauthorized withdrawals from their accounts.
4. Continues to work with its information security experts to assure that it is doing everything possible to protect the financial information of its clients.
5. Added new security features to its email accounts and strengthened its security monitoring.
6. Provided additional training to Wingate's staff on how to avoid the methods that unauthorized individuals used to gain access to its email.

In addition, each affected individual will be offered two years of identity theft protection services, at no cost.

Wingate notified three (3) New Hampshire residents via U.S. Mail, on April 10, 2019. A copy of the notice sent to the affected New Hampshire residents is attached.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,  
  
Matthew H. Meade

MHM/  
Enclosure



Wingate Wealth Advisors, LLC  
450 Bedford Street  
Lexington, MA 02420  
781-862-7100 Phone | 781-861-9707 Fax  
www.wingatewealthadvisors.com

April 10, 2019

Name  
Address  
City, State, Zip

**Re: IMPORTANT DATA SECURITY INCIDENT INFORMATION**

Dear [Name]:

We are writing to provide you information about recent email incidents at Wingate that may have affected your personal information. As a result of Wingate's investigation, we determined that some personal information that we maintained about some of our clients and their families as well as other information related to our business, our employees and related activities may have been accessed without authorization.

**At this time, we have no indication that any of your information has been inappropriately used by anyone.**

We take this matter very seriously because we know how important your personal information is to you. That is why we are providing this notice to you as a precautionary measure, to inform you of the incident and to explain steps that you can take to protect your information.

### **What Happened**

On February 1, 2019, we learned that a large number of emails had been sent from the account of one of our employees without authorization. We immediately notified our cybersecurity insurance company and began working with information security experts to determine what had happened and how. On February 5, 2019, we first learned that there had been incidents of unauthorized access to the employee's email account between January 9, 2019 and February 1, 2019. The Wingate employee had permission to access two other Wingate employees' accounts.

During the course of our investigation of the first incident we experienced a second incident that may have involved unauthorized access to two additional Wingate employee email accounts between February 19, 2019 and February 27, 2019. We conducted a comprehensive review of every email in the email accounts impacted by the first and second incidents to determine what specific information was in each email and who may have been affected.

### **What Information was Involved**

As a result of this review, we determined that personal information related to some Wingate clients and others was in the email accounts and may have been potentially affected including your name, address, financial account information, Social Security number, driver's license or other government identification. We are notifying you now because we found your information in at least one of the email accounts.

## **What We Are Doing About It**

Since we discovered these incidents, we have taken the following steps to enhance security and to help prevent something like this from happening again:

1. Reset the passwords of the impacted email accounts.
2. Notified Charles Schwab, Fidelity and TD Ameritrade, the three brokerage custodians which hold most of our clients' funds, of the incidents. They have placed all of our clients' accounts on a heightened security watch status and will alert us in the event of any unusual activities in any of our clients' accounts.
3. Confirmed that all three brokerage custodians which hold most of our clients' funds, have corporate policies that provide fraud protection for clients' accounts in the event of any unauthorized activity. The custodians' policy is to reimburse clients in the event of any unauthorized withdrawals from their accounts.
4. Continue to work with our information security experts to assure that we are doing everything possible to protect our clients' financial information.
5. Added new security features to our email accounts and strengthened our security monitoring.
6. Provided additional training to our staff on how to avoid the methods that unauthorized individuals used to gain access to our email.
7. Provided notice of this incident to appropriate state regulators.

## **What Can You Do**

We are notifying you so you can take additional actions to minimize or eliminate potential personal harm. **We strongly encourage you to take the following preventative measures to help detect and mitigate any misuse of your information:**

1. We are offering you a complimentary, two-year membership with Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks<sup>SM</sup> Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks<sup>SM</sup> Credit 3B, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.
2. Report any incidents of suspected identity theft to your local law enforcement and state attorney general.

As a precautionary measure, we advise you to take appropriate steps to protect your information. We recommend that you utilize the free credit monitoring service described above and remain vigilant to the possibility of fraud and identity theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity.

If you suspect unauthorized or suspicious activity, you can contact us and we recommend that you use the complimentary Identity Restoration service: [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, [www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html), by phone at 1 888 EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.

**For More Information**

You also may contact us with questions and concerns by contacting your advisor if you are a client or by emailing me at [jeff.white@wingatewealthadvisors.com](mailto:jeff.white@wingatewealthadvisors.com) or calling me at 781-862-7100.

We sincerely apologize for any inconvenience and concern this incident has caused you. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Sincerely,

A handwritten signature in black ink, appearing to be 'JH White', written in a cursive style.

Jeffrey H. White  
President

## EXPERIAN IDENTITYWORKS<sup>SM</sup> CREDIT 3B

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **July 17, 2019** (Your code will not work after this date)
2. VISIT the **Experian IdentityWorks website** to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
3. PROVIDE the **Activation Code**: [Code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number \_\_\_\_\_ as proof of eligibility for the identity restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)  
or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft). Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

### National Credit Reporting Agencies Contact Information

<b>Equifax</b> P.O. Box 105788 Atlanta, GA 303481 1-800-685-1111 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19022 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>
---	---	---

### Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

### STATE SPECIFIC INFORMATION

**MARYLAND residents:** You may obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This Office can be reached at:

Office of the Attorney General  
Consumer Protection Division  
200 St Paul Place  
Baltimore, MD 21202  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)  
(888) 743-0023

**NORTH CAROLINA residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice  
Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
[www.ncdoj.gov](http://www.ncdoj.gov)  
(877) 566-7226

**OREGON residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
[www.doj.state.or.us](http://www.doj.state.or.us)  
(503) 378-4400