May 23, 2014

**VIA USPS Certified Mail**

Hon. Joseph Foster
Attorney General
State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Placemark Investments, Inc. ("Placemark") is a registered investment adviser providing overlay management services for TD Ameritrade's Unified Managed Account Exchange program. Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, I am writing to notify your office of a recent data security incident that may have affected the security of seven (7) New Hampshire residents.

Specifically, in early April, Placemark learned that a malware program accessed one of Placemark's servers and directed it to send large batches of spam email. Security measures were taken immediately following the discovery of the malware to ensure that further unauthorized access would not occur, including changing the affected server's passwords. Placemark is implementing additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of Placemark's valued customers.

Based on a comprehensive analysis after a thorough investigation, we believe that the malware program's unauthorized access of the server had at least the potential to expose certain PDF documents tied to account creation that were stored on the server for short intervals. These PDF documents may have contained information relating to seven (7) New Hampshire residents' individual accounts, including names, addresses, dates of birth, and social security numbers. At this time, we have no reason to believe that any particular PDF document was exposed or that anyone has actually accessed a New Hampshire resident's personal information, nor do we have any reason to suspect that such personal information has been misused or will be misused in the future. However, as a precaution, we are notifying potentially affected individuals of the possible information security breach as required by law and to help safeguard them from potential misuse of their personal information.

Notices to the seven (7) potentially affected New Hampshire residents will be mailed between May 27, 2014 and May 30, 2014. In the notice, Placemark offers each potentially affected individual one year of free credit monitoring services from Experian. The notice also includes contact information for the three major credit reporting agencies, information on how to place a fraud alert or security freeze on their credit files, advice on preventing identity theft, and a Placemark telephone number that affected individuals may call to obtain further information about this data security incident. A sample copy of the notice being sent to consumers is attached.

Please do not hesitate to contact me if you have any questions regarding this incident or Placemark's response.

Sincerely,

Lauro Banda
Assistant General Counsel
Placemark Investments, Inc.
Phone: 972.404.8100 ext. 2031
Email: compliance@placemark.com

Attachment: Sample Notice

May 23, 2014

Customer Name
Address
City, State Zip Code

Re: **IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION**

Dear <Name of Customer>:

**Placemark Investments**, Inc. ("Placemark") is a registered investment adviser providing overlay management services for TD Ameritrade's Unified Managed Account Exchange program. As overlay manager, Placemark implements and coordinates the investment recommendations of one or more asset managers and/or mutual funds or ETFs selected by you for your account. You are a client of Placemark by virtue of your participation in TD Ameritrade's Unified Managed Account Exchange program.

We are writing to inform you of a recent data security incident that may have affected the security of some of your personal information. Specifically, in early April, Placemark learned that a malware program accessed one of Placemark's servers and directed it to send large batches of spam email. Security measures were taken immediately following the discovery of the malware to ensure that further unauthorized access would not occur, including changing the affected server's passwords. Placemark is implementing additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of Placemark's valued customers.

Based on a comprehensive analysis, we believe that this unauthorized access of the server had at least the potential to expose certain PDF documents tied to account creation that were stored on the server for short intervals. These PDF documents may have contained information relating to your account, including your name, address, date of birth, and social security numbers. At this time, we have no reason to believe that any particular PDF document was exposed or that anyone has actually accessed your personal information, nor do we have any reason to suspect that your personal information has been misused or will be misused in the future. However, as a precaution, we are informing you of the potential information security breach to help safeguard you from potential misuse of your personal information and to recommend ways for you to protect yourself. **Moreover, we have arranged for you to receive a complimentary one-year membership of Experian's® ProtectMyID® Elite.**

Experian's® ProtectMyID® Elite 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 PROTECTMYID® Now in Three Easy Steps**

1. ENSURE **That You Enroll By: August 15, 2014**
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide engagement #:

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:**

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, 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 877-441-6943.

We value and respect the privacy of your information. We hope that this letter and the enclosed *Steps You Can Take to Protect Yourself From Identity Theft* contain all necessary information, but please do not hesitate to call me at 800-266-7615, so that we can discuss any of your questions or concerns. We will work with you regarding any loss that you may have that is attributable to misuse of your personal information in connection with this incident. We wish that we could take the steps necessary to fully protect your information on your behalf, but some actions can only be authorized directly by you.

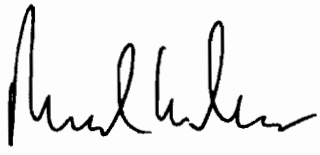
At Placemark Investments, we know that one of our most important responsibilities is to safeguard the personal information that you have entrusted to us. We maintain security standards and procedures that comply with federal guidelines and are designed to protect against unauthorized access

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.

or use. We continue to review and upgrade those practices as new risks emerge and industry standards and practices evolve. Even when unforeseen events occur, we want to make sure you are aware of the resources that are available to you to reduce any risk of misuse of your personal information, and we will work with you to minimize any inconvenience you may experience as a result of this incident. We believe that your personal information security has actually been compromised and that the actions suggested above are precautionary in nature. Please do not hesitate to call me at 800-266-7615 so that we may continue to assist you in any way we can.

Sincerely,



Richard K. Dion

President

Placemark Investments, Inc.

## Steps You Can Take to Protect Yourself From Identity Theft

1. **Review your account statements and credit reports and notify law enforcement and Placemark of suspicious activity.**

Even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 740241 | P.O. Box 9532 | P.O. Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1.888.766.0008 | 1.888.397.3742 | 1.800.680.7289 |

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

2. **Consider placing a fraud alert or a security freeze on your credit files.**

**Fraud Alerts:** There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed above.

**Security Freezes:** You may have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Security freeze laws vary from state to state.

Keep in mind that when you place the freeze, you may not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In addition, you may incur fees to place, lift and/or remove a credit freeze. The cost of placing, temporarily lifting, and removing a security freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you*

*must separately place a security freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit

**3. Learn more about how to protect yourself from identity theft.**

You may wish to review the Federal Trade Commission's guidance on how consumers can protect themselves against identity theft. For more information:

**Federal Trade Commission**
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft
1.877.ID.THEFT (1.877.438.4338)

**For Residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

**Maryland Office of the Attorney General**
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/idtheft
1.888.743.0023

**For Residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.gov
1.877.5.NO.SCAM (1.877.566.7226)