

RECEIVED

MAR 12 2019

CONSUMER PROTECTION

BakerHostetler

Baker & Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

March 11, 2019

VIA OVERNIGHT MAIL

Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Notice of Security Incident

Dear Attorney General MacDonald:

I am writing on behalf of our client, LPL Financial LLC ("LPL"), to notify you of a security incident that occurred at an LPL third-party service provider, Broadridge Financial Solutions, Inc. ("Broadridge").

Broadridge provides numerous financial institutions, including LPL, with client account management solutions that consolidate client information received by Broadridge from numerous third-party financial product sponsors, including AssetMark. Broadridge recently notified LPL that it inadvertently transferred AssetMark account data for 14 LPL clients to another broker-dealer's system between July 10, 2018 and January 8, 2019. As soon as the broker-dealer that received the data recognized the error, it immediately contacted Broadridge and took steps to ensure that the data was permanently deleted from its systems. The broker-dealer signed an attestation that the information transferred was permanently deleted, and was not copied, stored, used, retained, printed, or transmitted in any form. On February 12, 2019, Broadridge provided LPL with information identifying the LPL clients whose information was contained in the data files. LPL determined that the data files contained some personal information, including name, address, Social Security number, date of birth, AssetMark account number, and other AssetMark account-related information of one New Hampshire resident that has investments in variable annuities.

Today, LPL will mail a notification letter via U.S. first class mail to the one New Hampshire resident via U.S. mail in accordance with N.H. RSA § 359-C:20 4 in substantially the same form as the attached letter. LPL will offer the individual a complimentary one-year membership in a credit monitoring and identity theft protection service and will provide a telephone number for all notified individuals to call with any questions they may have.

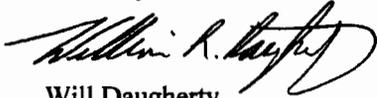
Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Gordon MacDonald
Office of the Attorney General
March 11, 2019
Page 2

To help prevent this type of incident from happening in the future, LPL will continue to work with Broadridge to evaluate ways to enhance its policies and procedures for its data transfers.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Will Daugherty", written in a cursive style.

Will Daugherty
Partner

Enclosure



March 8, 2019

Dear ,

LPL Financial LLC is the broker-dealer and custodian for accounts you maintain with your financial advisor, . In this role, protecting the privacy of your personal information is a top priority. We are writing to inform you about an incident involving some of your information and our third-party vendor, Broadridge Financial Solutions, Inc. ("Broadridge"). This notice explains the incident, measures we have taken, and some steps you can take in response.

Broadridge provides numerous financial institutions, including LPL, with client account management solutions that consolidate client information received by Broadridge from numerous third-party financial product sponsors, including AssetMark. Broadridge recently notified us that it inadvertently transferred AssetMark account data for 14 LPL clients to another broker-dealer's systems between July 10, 2018 and January 8, 2019. As soon as the broker-dealer that received the data recognized the error, it immediately contacted Broadridge and took steps to ensure that the data was permanently deleted from its systems. Upon learning this, we immediately began working with Broadridge to ensure the data was secure and started our own investigation to determine the scope of the information involved. On February 12, 2019, Broadridge provided us with information identifying the LPL clients whose information was contained in the data files. Our investigation determined that the data files contained some of your personal information, including your name, address, Social Security number, date of birth, AssetMark account number, and other AssetMark account-related information.

Although we have no indication that your information has been misused in any way, we want to make you aware of the incident and let you know that we take this seriously. Out of an abundance of caution, we are offering you a complimentary one-year membership of Experian's® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the pages that follow this letter.**

We apologize for any inconvenience or concern this incident may cause. To help prevent this type of incident from happening in the future, we continue to work with Broadridge to evaluate ways to enhance its policies and procedures for its data transfers. If you have any further questions regarding this incident, please call your financial advisor  directly at .

Sincerely,



Gerald F. Spada
Senior Vice President, Chief Privacy Officer



Activate IdentityWorks Credit 3B Now in Three Easy Steps

- Ensure that you **enroll by**: June 15, 2019 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: [REDACTED]

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 877-890-9332 by June 15, 2019. Be prepared to provide engagement number: [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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.

Additional Steps You Can Take

Regardless of whether you choose to take advantage of this free credit monitoring, we remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on your financial account, you should immediately contact your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of fraud alerts 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 ask 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 contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN 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.



Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.