



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

SEP 11 2017

CONSUMER PROTECTION

Christopher J. DiLenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienzo@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

September 6, 2017

VIA U.S. 1st CLASS MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Fiduciary Management, Inc. ("FMI"), 100 E Wisconsin Ave # 2200, Milwaukee, WI 53202, and are writing to notify your office of an incident that may affect the security of information relating to seven (7) New Hampshire residents, organizations and trusts. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, FMI does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On August 7, 2017, FMI discovered that the email account of one of its employees had been subject to unauthorized access earlier that day. FMI immediately terminated the unauthorized access and began an investigation with the assistance of a third party forensic investigator to understand and confirm the nature and scope of this incident. On August 11, 2017, the forensic investigator informed FMI that the available forensic evidence indicated the contents of the email account appeared to have been compromised. The forensic investigator confirmed that the email account is now secure, and that it was the only email account subject to unauthorized access.

While FMI's investigation is ongoing, information related to individuals, organizations and trusts for whom FMI managed brokerage accounts may have been present in the impacted email. The relevant data elements for individuals were their name, Social Security number the custodial bank or brokerage account number that FMI managed on the individual's behalf. For organizations or

trusts, the relevant data was the organization's or trust's name, Taxpayer Identification number, and the custodial bank or brokerage account number that FMI managed on its behalf.

Notice to New Hampshire Residents, Organizations and Trusts

On August 17, 2017, FMI began providing written notice of this incident to all affected individuals, which includes seven (7) New Hampshire residents, organizations and trusts. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and to Be Taken

Upon discovering the fraudulent nature of the email, FMI moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident. FMI is providing all potentially affected individuals access to two years of free credit and identity monitoring services with Experian. Additionally, FMI is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. FMI is also providing written notice of this incident to other state regulators as necessary. Further, FMI filed a complaint with the FBI.

FMI is in the process of reviewing its existing data security policies, procedures and staff privacy training, as well as identifying potential improvements to its existing security to reduce the risk of a similar incident from happening in the future.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very truly yours,



Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:ncl

Enclosure

EXHIBIT A



RE: Notice of Data Breach

Client:

We recently discovered suspicious activity related to one Fiduciary Management, Inc. (FMI) employee's email account that may impact your personal information or certain information related to your organization or trust. We immediately began an investigation, and as part of that investigation, we are working with third party forensic experts. We take this incident very seriously and write to provide you with the information that we know so that you may take steps to protect your information should you feel it is appropriate to do so.

What Happened? On August 7, 2017, we discovered that the email account of one of our employees had been subject to unauthorized access earlier that day. We immediately terminated the unauthorized access and began our investigation with the assistance of a third party forensic investigator to understand and confirm the nature and scope of this incident. On August 11, 2017, the forensic investigator informed us that the available forensic evidence indicated the contents of the email account appear to have been compromised. The forensic investigator confirmed that the email account is now secure, and that it was the only email account subject to unauthorized access.

What Information Was Involved? While our investigation is ongoing, your name, or your organization or trust's name, your Social Security number or Taxpayer Identification number, and the custodial bank or brokerage account number that FMI manages or managed on your behalf, may have been present in the impacted email account.

What We Are Doing. The confidentiality, privacy, and security of the information in our care is one of our highest priorities. We are in the process of reviewing our existing data security policies, procedures and staff privacy training, as well as identifying potential improvements to our existing security to reduce the risk of a similar incident from happening in the future. We have also reported this matter to law enforcement.

We are offering you two years of credit monitoring and identity restoration services from Experian. These services are designed to protect an individual's personal information from the possibility of identity theft. If your account with FMI was created with your Social Security number, you are eligible to receive the Experian services offered here. If your account with FMI was created with a Taxpayer Identification number, the organization or trust itself is not eligible for these services; however, an individual of your choosing can enroll himself or herself if so desired. More information about this product and enrollment information are below.

What You Can Do. We recommend that you contact your bank, brokerage firm or financial consultant to advise them of the possibility of a compromise of your account information and to ask them if there are any steps they would recommend be taken to monitor your financial accounts. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* which includes helpful guidance on the protection of personal information.

In addition, 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. 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 may have 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 offer is available to you for two years 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 web site.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary two-year membership. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: November 30, 2017** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
www.experianidworks.com/3bplus2
- Provide your **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 877-890-9332 by **November 30, 2017**. Be prepared to provide engagement number **DB03016** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-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.¹

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

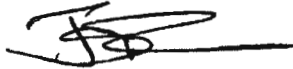
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** 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.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 for this information.

For More Information. Should you have any questions, please contact John Brandser at 414-226-4545.

Again, we take this incident very seriously and we apologize for any inconvenience or concern this may cause you.

Sincerely,



John S. Brandser
President

² 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.

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

The information about you in the email account can be used to prepare a fraudulent tax return. Therefore, we recommend that you contact your accountant and/or the IRS as soon as possible. You can visit the IRS website at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island Residents:** The Rhode Island Attorney General may be contacted at: Rhode Island Attorney General's Office, 150 South Main St., Providence, RI 02903. <http://www.riag.ri.gov>. Approximately 4 Rhode Island residents may have been affected by this incident. **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.