19854

WMS
The Open Family Office
1 Olympic Place, Suite 800
Towson, MD 21204

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter

Dear [Insert Recipient's Name]:

At WMS Partners, LLC ("WMS", "we", or "our"), protecting the security of the information in our possession is a responsibility we take very seriously. We are reaching out to inform you of a data security incident the firm experienced.

This letter explains the incident and the steps we have taken to address it. In addition, we will provide guidance on what you can do to further protect your personal information.

What Happened and What is Being Done

On December 21, 2020 at approximately 1:29 PM, one of our employees alerted the head of our IT staff that they had received a suspicious email sent from another one of our employees. Upon investigation, our IT department flagged the email as fraudulent and locked the compromised e-mail account. After a forensic audit by our third-party cybersecurity consultant, we were able to conclude that the bad actor gained access to the user's mailbox through the Outlook Web App ("OWA") for approximately ninety minutes, starting on or about 12:15 PM and concluding when we terminated access on or about 1:45 PM of that same day. We believe that the bad actor gained access to the employee's email account by way of a phishing email and then mistakenly accepting multi-factor authentication procedures designed to prevent unauthorized access to our systems.

From the information we have gleaned from the investigation led by our cybersecurity consultant, we know that no other WMS systems were accessed, that no bulk download of e-mails occurred, and that no searches were conducted from within the employee's e-mail account. We are, however, taking a conservative approach to our notification, based on the Private Identifiable Information ("PII") found within the employee's inbox.

While we regret that this situation occurred, it is an outlier in our operating history. We have and continue to provide employees with extensive training on the identification and prevention of cybersecurity threats, and this event would not have occurred but for lapses in the employee's observance of our cybersecurity protocols.

We have been diligently working with our outside information technology partners and our legal counsel on steps to take to notify you of this event and to ensure that this does not occur again. We have also worked with our partners at Schwab and TD Ameritrade to place increased scrutiny on all WMS accounts. For your reference, the employee in question no longer has access to any of our systems.

What Information Was Involved

The information that may have been accessed might have included personal information including your first and last names and financial account number(s). Please note that your social security number **was not** exposed as a result of this incident. **Additionally, we do not have any evidence that your information was actually viewed by the bad actor.**

What You Can Do

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify your financial advisor. If you suspect fraudulent activity or any incidence of identity theft, you should report it to the proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

Please see the "Steps You Can Take to Protect Your Information" insert provided with this notice for information on how you can further protect yourself. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. We have already communicated this matter to federal law enforcement and the relevant state authorities. We will gladly cover the cost of credit monitoring for affected individuals interested in such a service and are available to discuss any additional steps that you believe necessary.

What We Are Doing to Protect Your Information

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **XXXXXXX** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- 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 [customer service number] by **XXXXXXXX**. Be prepared to provide the engagement number **XXXXXX** 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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 [customer service number]. 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.

For More Information

At WMS, the privacy of your personal information is of the utmost importance to us. Please accept our sincere apology for this event. We deeply value our relationship with you. An advisor may have already spoken with you or left a voicemail. Should you wish to discuss this issue further, please feel free to reach out to us. We greatly appreciate your understanding.

Sincerely,

Todd M. Wickwire
Chief Executive Officer

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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 PROTECT YOUR INFORMATION
The following information is provided in accordance with certain state legal requirements.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. 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. For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. 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 19016
800-680-7289
www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. 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
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
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud 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. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

- For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
- For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
- For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.
For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.
For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.