



SCOT GANOW
937.641.2041
sganow@taftlaw.com

October 16, 2024

VIA EMAIL
CONFIDENTIAL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Weinberg Wealth Management, LLC

To Whom It May Concern:

In accordance with Maryland Code Ann. Com. Law §14-3501, et. seq., I am providing the following notice of a security incident on behalf of our client, Weinberg Wealth Management, LLC (“WWM”). A copy of the notice letter sent to the one Maryland resident is attached.

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH;

<u>Name:</u>	Scot Ganow
<u>Position:</u>	Outside Counsel for WWM
<u>Company:</u>	Taft Stettinius & Hollister, LLP
<u>E-mail:</u>	sganow@taftlaw.com
<u>Address:</u>	40 N. Main Street, Suite 900 Dayton, Ohio 45423
<u>Telephone number:</u>	937.641.2041

NAME AND ADDRESS OF THE BUSINESS THAT EXPERIENCED THE BREACH, AND THE TYPE OF BUSINESS;

Weinberg Wealth Management, LLC, 3333 Richmond Road, Suite 135, Beachwood, Ohio 44122 is a business that provides wealth and investment management services to its customers.

A GENERAL DESCRIPTION OF THE BREACH, INCLUDING THE DATE(S) OF THE BREACH, WHEN AND HOW THE BREACH WAS DISCOVERED, AND ANY REMEDIAL STEPS TAKEN IN RESPONSE TO THE BREACH;

On or about July 12, 2024, WWM first became aware of activity by a threat actor attempting to commit financial fraud. In order to attempt the financial fraud, the threat actor gained unauthorized access to one WWM employee's email account and a limited number of other WWM files (the "Incident"). Once aware of the Incident, WWM promptly took a series of actions to contain the Incident, remediate the issue, and launch an investigation. The investigation did determine this unauthorized access was limited to one employee account and did not affect other WWM accounts. However, WWM is not in a position to confirm whether the threat actors viewed or removed any client personal information as a result of this unauthorized access. WWM only knows that such access was possible.

Once aware of the Incident, WWM launched an investigation of the Incident, hired outside forensics experts to assist with understanding the impacts of the Incident, and promptly took a series of actions to contain and further remediate the Incident. WWM's remediation steps included, but were not limited to, sending alerts to potential recipients of fraudulent emails, quickly terminating any fraudulent access, working with its partners to prevent any unauthorized transfers, and successfully recovering any funds that were sent without authorization. With the forensic investigation complete, WWM commenced an analysis of the affected data files to determine what information was at risk. WWM also notified law enforcement of the Incident. Based on the forensic and cybersecurity experts' recommendations, WWM implemented both administrative and technical safeguards to further remediate the Incident and to prevent such an incident from occurring again. Beyond these immediate measures, WWM will continue developing its administrative, technical, and physical safeguards to further improve its security.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH;

WWM's investigation identified 1 individual with a Maryland address that may have been impacted. In the event that WWM determines any additional Maryland residents are impacted, WWM shall update this notice accordingly.

A DETAILED LIST OF CATEGORIES OF PERSONAL INFORMATION SUBJECT OF THE BREACH;

First name and last name, postal address, bank account information (including balances), driver's license number, date of birth, and Social Security Number.

THE DATE(S) THAT NOTIFICATION WAS/WILL BE SENT TO THE AFFECTED STATE RESIDENTS;

WWM expects to mail a letter to the impacted resident on or about October 16, 2024.

A TEMPLATE COPY OF THE NOTIFICATION SENT TO THE AFFECTED STATE RESIDENTS

Please see attached a substantially similar template copy of the notification sent to the resident.

WHETHER CREDIT MONITORING OR IDENTITY THEFT PROTECTION SERVICES HAS BEEN OR WILL BE OFFERED TO AFFECTED STATE RESIDENTS, AS WELL AS A DESCRIPTION AND LENGTH OF SUCH SERVICES; AND

Credit monitoring and identity theft prevention services have been offered via Experian for 24 months at no charge to the affected individual. The deadline for the individual to sign up for credit monitoring and identity theft prevention services is January 31, 2025. The affected individual is being provided an activation code and instructions detailing how to sign up for these services.

WHETHER THE NOTIFICATION WAS DELAYED DUE TO A LAW ENFORCEMENT INVESTIGATION (IF APPLICABLE).

WWM did not delay in sending notice. WWM became aware of the security incident on July 12, 2024. WWM engaged a trusted third-party forensics firm (“Forensics”) and legal counsel to assist in investigating the incident to better understand the scope and impact of the Incident. WWM completed its forensic investigations on or about September 20th, upon which WWM arrived at the conclusion that unauthorized access to personal information was possible. WWM completed its data analysis on or about September 30, 2024, and identified the individuals that required notice under applicable law and their respective states of residence.

[WWM Letterhead or Logo]

[Date]

[First Name Last Name]

[Address]

[City, State Zip]

RE: Notification of Security Incident

Dear [First Name],

Weinberg Wealth Management (“WWM”, “we” or “our”) takes the security and protection of your personal information seriously. We sincerely regret to inform you that an incident may have resulted in unauthorized access to your personal information. As shared below, our investigation leads us to believe the incident was focused on inducing individuals to complete fraudulent transactions and not personal information. Regardless, WWM is providing this letter to you out of an abundance of caution to provide you information about the incident and what you can do to remain vigilant and protect your personal information.

WHAT HAPPENED. On or about July 12, 2024, WWM first became aware of activity by a threat actor attempting to commit financial fraud. In order to attempt the financial fraud, the threat actor gained unauthorized access to one WWM employee’s email account and a limited number of other WWM files (the “Incident”). Once aware of the Incident, we promptly took a series of actions to contain the Incident, remediate the issue, and launch an investigation. The investigation did determine this unauthorized access was limited to one employee account and did not affect other WWM accounts. However, WWM is not in a position to confirm whether the threat actors viewed or removed any client personal information as a result of this unauthorized access. We only know that such access was possible.

WHAT INFORMATION WAS INVOLVED. While we have no evidence that any of this information was accessed by the threat actor, our forensic investigation and subsequent data analysis indicated that access to certain WWM data was possible and may have involved some or all of the following client personal information:

First and last name	Postal Address	Bank account information, including balances
Driver’s license number	Date of Birth	Social Security Number

WHAT WE ARE DOING. Once aware of the Incident, we launched an investigation of the Incident, hired outside forensics experts to assist with understanding the impacts of the Incident, and promptly took a series of actions to contain and further remediate the Incident. Our remediation steps included, but were not limited to, sending alerts to potential recipients of fraudulent emails, quickly terminating any fraudulent access, working with our partners to prevent the unauthorized transfers, and successfully recovering any funds that were sent without authorization. With the forensic investigation complete, we commenced an analysis of the affected data files to determine what information was at risk. We have also notified law enforcement of the Incident. Based on the forensic and cybersecurity experts’ recommendations, we have implemented both administrative and technical safeguards to further remediate the Incident and to prevent such an incident from occurring again. Beyond these immediate measures, WWM will continue developing its administrative, technical, and physical safeguards to further improve its security.

WHAT YOU CAN DO. While we have received no reports or indication of such activity, the risks related to unauthorized use of a Social Security number, government identification number, or financial

information may include identity theft, financial fraud, and tax fraud. Please be vigilant about monitoring your personal information, in particular your credit report information and financial accounts, to protect against fraudulent activity. Please also take care and attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf.

Although we have no evidence at this time that your information has been misused for fraud or identity theft as a result of this Incident, we are offering you **24 months of identity protection services and credit monitoring from a leading provider, Experian, at no charge.** These services help detect possible misuse of your personal information and provide you with identity protection support focused on identification and resolution of identity theft. For instructions on enrollment for these complimentary protection services, please refer to the instructions below.

If you have concerns about identity theft, you can also contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

FOR MORE INFORMATION. You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites. In some cases, fees may apply.

Equifax PO Box 740241 Atlanta, GA 30374 800-525-6285 www.equifax.com	Experian PO Box 4500 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion PO Box 2000 Chester, PA 19016 877-322-8228 www.transunion.com
--	--	--

Credit Reports. You can request credit reports from all three credit bureaus be sent to you free of charge. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Security Freeze. Under state law, a security freeze (or a credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

Your full name	Date of Birth	Social Security number
Postal address	Email address	Other information the Credit Reporting Agency may require.

The credit bureaus have one (1) business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three (3) business days. The credit bureaus must also send written confirmation to you within five (5) business days.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities 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. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one (1) hour. If you request the thaw by regular mail, the credit bureaus have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC at: Federal Trade Commission, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-6000.

<u>For New York Residents:</u> You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: (800) 771-7755 Website: https://ag.ny.gov/	<u>For Maryland Residents:</u> You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 200 St. Paul Place Baltimore, MD 21202 Phone: 410-528-8662 Website: https://www.marylandattorneygeneral.gov/
--	--

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at:

Contact: Grant Dinner
Email: [EMAIL ADDRESS]
Telephone: [TELEPHONE NUMBER] & [TOLL FREE NUMBER]
Address:

Weinberg Wealth Management, LLC
3333 Richmond Road, Suite 135
Beachwood, Ohio 44122

Sincerely,

Grant Dinner
Weinberg Wealth Management, LLC

Experian IdentityWorksSM

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident 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 occurred from the date of the incident (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 Identity Restoration is available to you for 24 months 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. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by January 31, 2025, 5:00 pm Central Time**. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 931-7577** by January 31, 2025 (5:00 PM Central Time). Be prepared to provide engagement number B133404 as proof of eligibility for the Identity Restoration services by Experian.

Home

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. *
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.