

Office of the Attorney General
ATTN: Security Breach Notification
Baltimore, Maryland 21202

December 12, 2024

Dear Maryland Attorney General's Office,

We are writing to notify you of a data security incident involving Maryland residents. Please find a summary of information regarding the unauthorized breach below.



Approximate Date of the Incident and How the Breach was Discovered:

The data breach occurred between October 21 to October 25, 2024. The breach was discovered by our information technology vendor in conjunction with our Director of Operations in early November.

Cause of Breach:

The data breach was the result of an employee's interaction with a targeted spear fishing email. This interaction occurred while the employee's dual-factor authentication security was temporarily disabled for Microsoft Office 365. The employee's log-in credentials were captured by the phishing email. An unauthorized individual was able to access the employee's email inbox, which contained personal information about our clients.

The dual-factor authentication for the employee's access to the firm's virtual private network (VPN) was not disabled and therefore the unauthorized individuals were not able to gain access to our network folders.

Number of Maryland Residents:

As known at the time of this notification, the data security incident involved 80 individuals residing in Maryland. There was only one Maryland resident whose client's name, social security number, and date of birth could have potentially been obtained by the unauthorized individual. The breached personal information for the remaining 79 Maryland residents was limited to their names, email addresses, and financial institution account numbers. We are not aware of any resulting identity theft, fraud, or financial losses to the consumers.

Steps Taken to Remedy Breach:

The employee's log-in credentials were changed, and the dual-factor authentication for gaining access to Microsoft Office 365 was reestablished. Going forward, the IT vendor will continuously monitor the security settings of all the employees to ensure their dual-factor authentication status is active. The firm has met with its IT vendor three times since the breach and is working on identifying and implementing additional cyber security measures.



Sample of the Notification to Affected Parties:

Dear Rosanna,

We want to bring to your attention a recent cybersecurity issue that occurred within Evermay. There have been targeted "phishing scams" where unauthorized individuals could have potentially obtained your name, email addresses, social security number, date of birth, account number for Charles Schwab and other financial institutions that were provided to us. Based on our IT vendor's extensive review, no data was extracted from our network folders.

If you receive an email appearing to be from Evermay, especially one containing attachments or links, and are not expecting an email from us, please give us a call to verify the authenticity of the communication.

Please be sure to utilize your Evermay Client Portal to transmit any sensitive information, including credentials, bank account information, social security numbers or other non-public personal information. We also recommend updating your Charles Schwab password routinely.

Evermay has taken extensive measures to enhance our cybersecurity protection, including ongoing efforts to identify and address suspicious activity.

We sincerely apologize for any worry or inconvenience this incident may cause. Please be assured that we take information privacy very seriously and are committed to protecting your personal information. If you have any questions or concerns, please do not hesitate to contact your Evermay team at 703-822-5666.

Best Regards,
Damon

Damon A. White
Chief Operating Officer & Co-Founder
P: (703) 822-5696 | F: (703) 312-1110
evermaywealth.com

EVERMAY
A Richter Life

The information contained in this email (including any attachments) is privileged and confidential and intended solely for the use of the intended recipient(s) and may contain proprietary information. If you have received in error, please notify the author by replying to this email and delete the email and attachments immediately. Message transmission is not guaranteed to be secure. This message does not constitute, tax or legal advice, or an offer or solicitation with respect to the purchase or sale of any security in any jurisdiction in which such offer or solicitation is not authorized or to any person to whom it would be unlawful to make such offer or solicitation. Past performance does not guarantee future results. No representation, guarantee or warranty is provided as to the correctness, completeness or timeliness of information provided in this message, which information may be based upon assumptions, may change without notice and should not be relied upon in making an investment decision. Evermay Wealth Management LLC does not accept any liability whatsoever for any direct, indirect or consequential loss arising from any actions undertaken in reliance on the content of the email or its attachments.

We plan to contact the affected clients in the coming days with contact information for the major consumer reporting agencies, the Federal Trade Commission and the Office of the Attorney General.

Please contact me if you have any questions.

Regards,



Kris L. Sumner
Chief Compliance Officer
Evermay Wealth Management, LLC
(703) 576-8609

