

April 12, 2022

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Data Security Event:

Dear Attorney General Frosh,

PlanMember Securities Corporation (“PlanMember”) is submitting this notice to provide the Maryland Attorney General with information regarding a suspected cybersecurity event involving unauthorized access to consumer personal information (“PI”) pursuant to Md. Code Ann. Comm. Law 14-3504.

PlanMember has retained outside counsel and is in the process of retaining a leading forensic firm to investigate the incident and ensure that the issue is resolved. The investigation is ongoing, and the below represents our understanding of the events based on PlanMember’s investigation to date.

PlanMember is a dually registered broker-dealer and investment adviser and an insurance producer specializing in products for educators nationwide. PlanMember is registered in all 50 states and the District of Columbia and is headquartered in California. As the investigation progresses, we are communicating about this incident with our regulators across our business lines.

On February 17, 2022, PlanMember’s Chief Financial Officer received a phishing email which appeared to be from PlanMember with an attachment disguised as an audio file. When opened, the attachment produced a field requesting his username and password, which he provided. A “page not found” screen appeared and the CFO closed the email.

The attackers appear to have captured his email account login information and established rules in the CFO’s email account to hide certain communications while they set up a business email compromise (BEC) fraud scheme.

On March 15, 2022, an employee received a request that appeared to be from the CFO asking her to pay two invoices, one for \$100,000 and the other for \$900,000. The employee brought them to the CFO, who did not recognize them. At that point, the CFO directed the firm’s IT department to investigate. The IT department identified email account rules that directed certain outgoing emails to a file location other than the sent mail box, and incoming emails from certain email addresses to other files locations rather than his inbox. This included rules designed to hide correspondence with the firm’s bank through which the attackers attempted (unsuccessfully) to change the authorized signors on the account.

The initial investigation produced no evidence of additional attacker activity. However, in the CFO’s account were emails containing at least two attached documents containing employee and client personal information in the form of Social Security numbers, account numbers, and names. It is unknown at this time whether the attackers accessed these emails or their attachments. PlanMember is also currently investigating how the attackers were able to work around the two factor authentication protecting the email account.

Once this incident was detected, PlanMember quickly took a number of steps to protect the firm and its clients, including:

- changing passwords;
- alerting its bank to the malicious activity;
- creating new alert mechanisms to identify any automated email rules to outside email addresses;
- conducting an initial review of the CFO's email account to identify any personal information or other sensitive information which may have been subject to unauthorized access;
- searching within the firm to identify any other individuals who may have received the phishing email;
- examining the CFO's laptop for any malicious code;
- contacting the firm's cyber insurance carrier;
- retaining outside counsel with an expertise in cybersecurity; and
- retaining a leading forensic firm, through outside counsel, to investigate the incident and ensure that the issue is resolved.

On March 30, upon discussion with outside counsel and based on findings of our initial investigation, we determined that this incident constituted a notifiable security incident.

PlanMember is continuing its investigation to determine the scope of impact of this incident, including identifying individuals who may have been affected and their states of residence. PlanMember will update you and other regulatory agencies as the investigation progresses. Although PlanMember is unable to determine whether all potentially affected individuals actually had personal information affected, PlanMember is erring on the side of being over-inclusive in determining who may have been affected. Based on its investigation to date, PlanMember believes 1,348 Maryland residents may have been affected, however PlanMember is still working to determine the full extent of the impact of this incident. PlanMember plans to notify individuals once the potentially affected individuals have been identified and will provide free identity theft protection services. PlanMember also intends to notify consumer reporting agencies.

Should you have any questions please do not hesitate to contact our outside counsel: Michael Bahar (MichaelBahar@eversheds-sutherland.com or +1.202.383.0882) or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).

Sincerely,

Sean Haley, Chief Compliance Officer
PlanMember Securities Corporation



[6187 Carpinteria Ave]
[Carpinteria, CA 93013]

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

[Date]

Re: Notice of Data Security Incident Involving Your Personal Information

Dear [First Name] [Last Name],

At PlanMember Financial Corporation, ("PlanMember") we take privacy very seriously. It is therefore important that we make you aware of any data privacy issues that may affect you. Below you will find information about an incident that may have impacted your personal information.

We are actively taking steps to protect your information as outlined below.

What Happened

On March 15, 2022, PlanMember observed anomalous activity on our IT network. We launched an investigation and took a series of immediate steps designed to remediate the issue. PlanMember then engaged with a leading incident response and forensics firm to further secure our systems, determine the root cause, and further protect your information. PlanMember also reported the event to law enforcement.

PlanMember appears to have been targeted by criminal actors with the intent of stealing funds from PlanMember's corporate account. To effect their fraud scheme, the criminal actors illegally gained access to an executive's email account and impersonated him in an unsuccessful attempt to route funds to criminal-owned bank accounts. Within the executive's email account were emails containing at least two attached documents containing employee and client personal information in the form of Social Security numbers, account numbers, and names. It is unknown at this time whether the attackers accessed these emails or their attachments. Out of an abundance of caution, however, we are providing you notice in case this information was accessed.

What Information Was Involved

Our records indicate that your name, Social Security number, and PlanMember account number may have been accessed.

Actions We've Taken to Safeguard Your Information

We take our responsibility to safeguard your personal information very seriously. We have engaged with a leading cybersecurity company to investigate the incident and further protect your information, and we have implemented processes and protocols designed to mitigate this type of activity.

Identify Theft Protection Service

To help protect your identity from misuse, we are offering complimentary access to Experian IdentityWorksSM for 12 months. This product provides you with superior detection and resolution of identity theft. 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 one-year membership.

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

- Ensure that you **enroll by:** (Your code will not work after this date.)
- **Visit** Experian's website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code:** [Activation Code]

Please do not share this information as these links are exclusive to you and your account.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian's® IdentityWorksSM online, please contact Experian's customer care team at (855) 726-7329 by June 30, 2021. Be prepared to provide engagement number [] as proof of eligibility for the Identity Restoration services by Experian.

Steps You Can Take for Identity Theft Protection

We encourage you to take advantage of Experian's® IdentityWorksSM identity theft protection services at no cost to you. In addition, there are other steps you may take to further protect yourself against identity theft or other unauthorized use of your personal information. Information regarding these steps is provided on the attached pages entitled "*Steps You May Take to Protect Yourself Against Potential Misuse of Information.*"

Contact Information

We wanted you to know the nature and extent of this incident and to make you aware of the steps we are taking to protect your information. If you have questions about anything contained in this letter, please contact us by phone at [].

Regards,

Sean Haley, Chief Compliance Officer
PlanMember Securities Corporation

Steps You May Take to Protect Yourself Against Potential Misuse of Information

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

Fraud Alerts: There are also two types of fraud alerts that 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 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must*

separately place a credit freeze on your credit file at each credit reporting company. Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of the District of Columbia: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, <https://oag.dc.gov/>.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of New York: You may also obtain information about security breaches and preventing and avoiding identity theft from the New York Office of the Attorney General: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Oregon: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.

For residents of Rhode Island: You also may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150 South Main Street, Providence, RI 02903, (401)-274-4400, <http://www.riag.ri.gov>. You may also be able to file or obtain a police report about this incident.

July 1, 2022

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

Re: Data Security Event Update:

Dear Attorney General Frosh,

PlanMember Securities Corporation (“PlanMember”) is submitting this notice to update our April 12, 2022 notification of a cybersecurity event involving unauthorized access to consumer information.

Our investigation is now complete. The facts as we now know them are as follows:

On February 17, 2022, PlanMember’s Chief Financial Officer received a phishing email, which was disguised as a voicemail-to-email transcription and which contained a malicious embedded URL. The email was spoofed to appear as if it came from a PlanMember account. The embedded URL claimed to link to an audio recording of the message. While the malicious URL was no longer accessible at the time of the investigation, it appears likely that the URL hosted a phishing page which resembled a legitimate Microsoft O365 service, and produced a field requesting the CFO’s username and password, which the CFO provided. He then received an SMS-based multi-factor authentication (MFA) code on his mobile device, as well as a prompt to enter his MFA code, which he provided. A “page not found” screen appeared and the CFO closed the email. Having captured his email account credentials and MFA code, the attackers were able to access the web-based version of his Microsoft Office 365 email account.

The threat actors then attempted two separate instances of financial fraud.

First, between February 17 and February 18, the threat actors contacted PlanMember’s corporate bank using the CFO’s compromised email account and attempted to add a signor, “Alan Myers,” to the account and to remove the other executives from the bank account. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

The second fraud attempt occurred on March 15. The threat actors created a fake email thread using the identity of a real PlanMember employee in the Human Resources department that frequently handles invoices, showing a trail of communication between PlanMember and a fake investment

company. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

PlanMember then retained outside counsel with expertise in cybersecurity incidents and, through counsel, a leading cyber forensic firm to investigate the root cause and the actions that the attackers took, which are described above.

The forensic review determined that the intrusion was limited to the CFO's email account; no additional compromised systems or employee accounts were identified. Moreover, the investigation determined that the threat actors did not download or sync the mailbox to a local client, and that the threat actors did not access the SharePoint or OneDrive documents associated with the CFO's Office 365 account.

Nonetheless, during its initial review, PlanMember identified client and employee PII in the form of names, Social Security Numbers, and account numbers in attachments within the CFO's email inbox. At the conclusion of the forensic investigation, PlanMember's counsel reviewed potentially impacted documents and identified those containing employee and client personal information in the form of names, Social Security numbers, and account numbers. There were also limited instances of driver's license numbers and the COVID-19 vaccination status for certain employees.

There is no indication that any of this data was accessed, and the forensic evidence indicates that the attackers were likely solely motivated to divert corporate funds, not exfiltrate and misuse personal information. However, out of an abundance of caution, PlanMember is notifying all potentially impacted individuals that they have identified, totaling 96,813 individuals, including 1,660

potentially affected individuals in Maryland, and providing them with free identity theft protection services. The individual notification letters will be mailed on July 1.

PlanMember has made the following changes to further enhance the security of its information systems:

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] oted file

PlanMember is also modifying its internal policies regarding how certain data types may be stored, and to sweep its system to identify where PII or other sensitive data exists.

Should you have any questions please do not hesitate to me at MichaelBahar@eversheds-sutherland.com or +1.202.383.0882, or my colleague Alexander Sand at AlexanderSand@eversheds-sutherland.com or +1.512.721.2721.

Sincerely,

Michael Bahar
Partner
Eversheds-Sutherland (US) LLP