EVERSHEDS SUTHERLAND

Eversheds Sutherland (US) LLP
700 Sixth Street, NW, Suite 700
Washington, DC 20001-3980

April 1, 2022

Cyber Incident Event Description

PlanMember Securities Corporation ("PlanMember") is submitting this notice to provide the New York State Department of Financial Services ("DFS") with information regarding a suspected cybersecurity event involving unauthorized access to consumer nonpublic information pursuant to 23 NYCRR § 500.17. 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.

EVERSHEDS SUTHERLAND

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 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.

The investigation is ongoing. PlanMember will update NY DFS and other regulatory agencies as the investigation progresses. 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).