Appendix

Outcomes One, Inc. ("Outcomes") recently completed an investigation related to an email phishing incident that occurred on July 1, 2025. The affected employee noticed suspicious activity in his Outcomes email account and reported it to the Outcomes security team, which promptly took action to secure the account and engaged third-party specialists to help investigate the matter. No other email accounts were involved in this incident.

During approximately one hour of unauthorized access to the account, various files and emails were accessed. Although the focus of the unauthorized individual's activities appeared to be related to financial information, not information related to health plan members or patients, Outcomes performed a data review to determine if any of the accessed items contained individuals' information. On July 17, 2025, Outcomes determined that one of the items that could have been accessed by the unauthorized individual included individuals' names and one or more of the following: medical provider names, health insurance information, and medication information.

Beginning on July 25, 2025, Outcomes started notifying the data owners of the incident. Outcomes worked with the data owners to provide them with information regarding the investigation, the information involved in the incident and the impacted individuals. Thereafter, the data owners delegated to Outcomes, as a HIPAA Business Associate, the notifications to be made to members/patients on behalf of the covered entities.

On September 23, 2025, Outcomes mailed a notification letter via U.S. First-Class mail to 3,477 Washington residents whose information was involved, in accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*) and/or Wash. Rev. Code § 19.255.010. A copy of the notification is enclosed. Outcomes has provided a toll-free call center to answer any questions notified individuals may have. The attachment to this letter shows the Outcomes client on whose behalf Outcomes is notifying and the number of residents who are being notified pursuant to state law.

Outcomes took immediate steps to identify and contain this incident and will continue to evaluate enhanced safeguards and security measures to further protect its email system and reduce the likelihood of a similar future event.

Client	Total – WA Residents
Aetna Health Insurance Company	3477

Outcomes

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Outcomes One Inc. ("Outcomes") works with health plans to provide their members with medication therapy management ("MTM") and medication adherence services. We are committed to protecting the privacy and security of information in our care. We are writing to notify you about an incident that involved some of the information we received related to the services we provide to your health plan, Aetna Health Insurance Company. This letter explains the incident, the measures we have taken, and steps you may consider taking.

What Happened?
We recently completed an investigation related to an email phishing incident that occurred on July 1, 2025. The affected employee noticed unusual activity in his Outcomes email account and reported it to the Outcomes security team, which promptly took steps to ensure the account was safe and hired an outside specialist to help investigate the matter. No other email accounts were impacted by this incident.

What Information Was Involved?
During about one hour of unauthorized access to the account, various files and emails were accessed. We performed a data review to determine if any of the accessed items contained your information. On July 17, 2025, we determined that one of the items that may have been accessed included your name and one or more of the following: demographic information, medical provider name, health insurance information, and medication information. Note that Social Security numbers were **not** involved.

What We Are Doing.
We take this matter very seriously. To help prevent a similar incident, we have added and will continue to evaluate enhanced safeguards and security measures to further protect our email system, and we have added enhanced employee training regarding phishing emails.

What You Can Do.
It is always a good idea to remain vigilant and review statements you receive from your health plan and health providers. If you identify charges for services or medications you did not receive, you should contact your health plan immediately.

For More Information.
We have set up a designated incident response line to answer your questions. You can call 877-332-1681, Monday through Friday, 9:00 AM to 9:00 PM Eastern Time, except for major U.S. holidays. We remain committed to protecting the confidentiality and security of the information in our care and apologize for any concern or inconvenience this may cause.

Sincerely,

Outcomes