

September 29, 2026



Manav Choudhary

Dear Mr. Choudhary,

I am writing on behalf of Wispr AI's security team to acknowledge and thank you for your participation in our responsible disclosure program. This letter is intended as a statement of appreciation for your engagement, effort, and conduct throughout the process, and is not a certification of finding severity, a confirmation of remediation, or a bounty award notice.

Between August 29 and September 21, 2026, you submitted four vulnerability reports spanning four distinct vulnerability classes: an authentication bypass in a desktop protocol handler, an improper access control issue in enterprise domain-join, an update-channel integrity weakness, and cleartext storage of sensitive data at rest. All four were confirmed as valid security findings. Before beginning any testing you contacted our security team to confirm the program was active and to obtain its scope and rules of engagement, and all of your testing was conducted against accounts you created yourself.

The quality of your methodology was consistently high. Every report carried a CVSS 3.1 vector, a CWE classification, reproducible steps, disclosed test windows with time zones, and two independent evidence files. One report included a documented control test across four unclaimed domains, demonstrating the underlying mechanism rather than asserting it. On that same report a Wispr engineer independently reproduced both of your demonstrations and confirmed the underlying issue, noting at the time that your evidence files made it quick to validate, and that this is not always the case. You later returned to that finding unprompted with a substantial additional evidence package, establishing that the exposure reached considerably further than your original report had shown.

Most notably, you documented a negative result against your own interest. In testing whether the elevated access you had found could reach other members' content, you established that those endpoints were correctly scoped and reported that limitation explicitly — narrowing the assessed impact of your own finding and weakening your own severity argument in the process. Researchers rarely volunteer the boundary of their own work, and it is the part of this engagement we found most creditable.

Your disclosure conduct matched that standard. When asked on September 1 to hold public disclosure pending confirmed remediation, you agreed and honored it, and you confirmed in writing that you had read no real customer's data and modified no records belonging to others. Where our severity assessments differed from your own, you argued your position on methodology and evidence, without pressure, deadlines, or threat of disclosure. We are grateful for the rigor and care you brought to this program, and we wish you continued success in your studies and in your career in cybersecurity.

Sincerely,

A handwritten signature in black ink, appearing to read "J Scot".

Jason Scot
Wispr Senior Technical Support and Compliance Engineer
Wispr AI