Airwallex

Dear Chairman Moolenaar:

I write in my capacity as an advisor to Airwallex to transmit the attached letter from Jack Zhang, the company's Co-founder and Chief Executive Officer, responding to your September 17 letter to Secretary Bessent.

I have spent a career, across two administrations and in private practice since, dealing with questions your Committee exists to address. I would note, respectfully, where I believe this matter originated: not with a regulator's finding, an intelligence referral, or a breach, but with concerns first raised publicly by a board member of a direct competitor. Given this, I would hope this matter is handled with the independent judgment it deserves.

I would also note that the Committee's technical analysis found no covert data-exfiltration channels, no hidden PRC infrastructure, and no obfuscated communications, and the letter itself states plainly that the Committee has not concluded Airwallex engaged in unlawful conduct. Those are significant facts, and they belong at the center of how this matter is understood, not as a footnote.

Mr. Zhang's letter fully responds to the concerns expressed in your letter. Airwallex has been transparent on these issues and will continue to be. I would welcome the opportunity to discuss this with you or your staff directly.

Respectfully,

William P. Barr

September 18, 2026

The Honorable John Moolenaar
Chairman
House Select Committee on the Chinese Communist Party
246 Cannon House Office Building
Washington, DC 20515

Dear Chairman Moolenaar,

I am writing in response to your September 17 letter to Secretary Bessent regarding Airwallex.

For months, Airwallex has been the target of an aggressive and increasingly conspiratorial campaign questioning our company, our people and the security of our customers' data. Your letter raises a number of factual inaccuracies and inferences that I believe warrant a direct response.

The origins of these allegations did not begin with evidence of a security breach, a finding by a regulator or a concern raised with us by a national-security agency. The source of these claims is a prominent and politically connected Silicon Valley venture capitalist who serves on the board of a direct Airwallex competitor. Airwallex is an Australian company, co-headquartered in San Francisco, building a significant business in the United States and competing directly with some of Silicon Valley's best-funded fintech companies.

We welcome rigorous scrutiny of financial institutions entrusted with sensitive American data. But that scrutiny should be grounded in evidence, applied consistently across the industry and focused on the questions relevant to national security, including where data is stored, who can access it and what technical controls protect it.

On those questions, the facts are clear. U.S. customer data is stored in the U.S. Like other global financial institutions, we have staff based in China and Hong Kong because we operate globally and these are important markets. But those staff cannot access U.S. customer data. This goes beyond what the U.S. government requires of global companies.

Access is restricted under strict least-privilege controls, protected by phishing-resistant multifactor authentication and continuous monitoring. We asked Coalfire, an A2LA-accredited FedRAMP Third-Party Assessment Organization, to independently examine those controls. It found our security program "intentional, structured, and forward-looking," with controls that "go beyond minimum expectations."

Since these allegations first surfaced, I have personally met with dozens of officials across the Administration and Congress, including Senator Cotton's staff and members and staff of the House Select Committee on China. We have discussed our ownership, technology architecture, security controls, and data governance program in detail. These conversations have left leaders and their staff confident in our controls.

Indeed, your own letter acknowledges that the Committee's technical analysis found "no covert data exfiltration channels, no hidden Chinese-infrastructure endpoints, and no obfuscated communication patterns." It also states explicitly that the Committee has "not reached the conclusion that Airwallex has engaged in unlawful conduct."

Against that backdrop, some of the letter's characterizations are particularly troubling. Its discussion of our workforce, for example, combines corporate records, historical global headcount figures and what the letter itself calls "less reliable" employment-site data to suggest that as much as 75 to 94 percent of our workforce could be based in mainland China. That is completely inaccurate. Airwallex employs more than 2,700 people across 27 offices globally. Today about a quarter of our workforce is based in China. More importantly, the location of employees is not evidence of access to American customer data.

Airwallex was founded in Melbourne in 2015 because we believed businesses of every size should have access to financial infrastructure once reserved for the world's largest corporations. A decade later, we are proud of what that has meant for Australian businesses. Independent research by Mandala Partners released this week estimates that businesses using Airwallex generated $4.6 billion in economic benefits in Australia in 2025, supporting economic activity equivalent to roughly 29,000 full-time jobs.

We want to create that same opportunity for American businesses: helping companies founded in the United States compete, hire and grow globally with world-class financial infrastructure behind them.

We understand that earning the trust required to do that carries serious responsibilities. We accept them. We will continue to cooperate with policymakers and regulators, subject our systems to independent scrutiny and invest heavily in security. But scrutiny must be factual and consistent.

We are proud to be part of a generation of rapidly growing fintech companies born outside the United States, including Wise, Adyen and Nubank, that set out to solve the real cost and complexity faced by businesses and people trying to trade, pay and grow across countries. What we share is an ambition to become infrastructure, not simply a middleman. That means applying for licenses, submitting to regulatory examinations, building direct relationships with central banks and earning the trust of governments market by market.

Airwallex's investors include some of the most respected institutions in venture and global finance, including Addition, Greenoaks, T. Rowe Price, Lone Pine Capital, Salesforce Ventures, Visa and Mastercard. Tencent also holds a passive minority stake of less than 10 percent, with no board seat and no information rights beyond those of any passive minority shareholder.

I was born in China. I cannot change that fact, nor would I seek to. I am a proud Australian citizen. I arrived in Melbourne as an immigrant at fifteen with little English and no safety net, and Australia gave me the education, the opportunity and the freedom to build something. The United States represents that same promise, perhaps more powerfully than anywhere else on earth. It is the place where the world's best companies come to prove themselves, and it is the place I came to build Airwallex's future.

Serving the U.S. market means competing in one of the most demanding financial services environments in the world. We knew that going in and we welcomed it. Sophisticated investors, enterprise clients and heavily regulated financial partners do not take our word for it. They conduct rigorous due diligence on our licenses, our security practices and our data flows. Our regulators examine us. We earn their business because we welcome that scrutiny and stand up to it.

Airwallex should be held to a high standard. So should every global bank, payments company and fintech entrusted with American data. National-security policy should reflect those standards, not the competitive interests of powerful participants in Silicon Valley.

I would like to renew my invitation to meet with you directly and provide the Committee with the technical evidence, independent assessments and factual corrections necessary to evaluate these questions on their merits.

Sincerely,

Jack Zhang
Co-founder and Chief Executive Officer
Airwallex