Kip Meek Chair, Cloud Services Market Investigation Competition & Markets Authority 25 Cabot Square London E14 4QZ

By Email

99 Bishopsgate London EC2M 3XF United Kingdom Tel: REDACTED Fax: REDACTED www.lw.com FIRM / AFFILIATE OFFICES Austin Milan Beijing Munich Boston New York Orange County Brussels Century City Paris

Rivadh

Seoul

San Diego

San Francisco

Silicon Valley

Washington, D.C.

Singapore

Tel Aviv

Tokvo

Chicago

Düsseldorf

Frankfurt

Hamburg

London

Madrid

Hong Kong Houston

Los Angeles

Dubai

8 August 2024

Dear Kip,

Re: CMA Cloud Services MIR – Identity and Access Management Follow-up

A theme that runs through the responses to the CMA's working paper on technical barriers, including Microsoft's own, is the complex nature of interoperability that invariably requires some level of effort in making various components of a system, even if developed by the same vendor, work together. Such claims can be superficially persuasive against a backdrop where integration of any kind requires effort, and as Microsoft acknowledges in its own response to the Technical Barriers Working Paper, features inherent friction. It is, however, important that the CMA has the necessary detail and full context to ensure that it is able to properly assess any evidence it is being provided.

Over the course of the CMA's market investigation, the CMA has occasionally asked questions regarding identity and access management ("*IAM*") solutions, including Microsoft Entra ID. Upon reading Google's response to the Technical Barriers Working Paper and reflecting on recent questions from the CMA, Microsoft is concerned that the CMA may not be receiving accurate information as it relates to IAM services and Microsoft's solutions in particular. This letter seeks to address a few of the most inaccurate representations. Microsoft would be pleased to discuss IAM in more detail if the CMA has any remaining questions or concerns.

As the CMA has observed, inherent in any cloud deployment is the need to manage identity and permissions for the cloud resources being accessed. Each cloud vendor must be certain that only authorized individuals and accounts access cloud resources of their customers and identity solutions are critical in this respect. The work needed to make identity authentication work when deploying cloud services from multiple vendors is a scenario that is wellunderstood by enterprises and commonly solved using *"federation*" between service providers.¹ This issue arises whenever enterprises deploy cloud services from multiple

¹ See Technical Barriers Working Paper, paras. 6.27.

Latham & Watkins is the business name of Latham & Watkins (London) LLP, a registered limited liability partnership organised under the laws of New York and authorised and regulated by the Solicitors Regulation Authority (SRA No. 203820). A list of the names of the partners of Latham & Watkins (London) LLP is open to inspection at its principal place of business, 99 Bishopsgate, London EC2M 3XF, and such persons are either solicitors, registered foreign lawyers, or managers authorised by the SRA. We are affiliated with the firm Latham & Watkins LLP, a limited liability partnership organised under the laws of Delaware.

vendors, such as customer relationship management, staff management, or finance and accounting applications. Contrary to Google's claims that Microsoft deliberately impedes interoperability,² there are multiple IAM service providers, including Google, competing on the quality and ease of implementation of their IAM services and especially in how they integrate with such cloud services from a broad range of providers – including Microsoft. In short: in IAM, interoperability is a *feature* of competition.

Similarly, as enterprises migrate from on-premises Active Directory solutions to cloud IAM services, IAM service providers offer competing solutions to help enterprises with migration or hybrid deployments. Google's claim that "*Microsoft does not provide the necessary interoperability information for third-party cloud IAM solutions to integrate effectively with Active Directory*"³ is, simply put, wrong. Microsoft publishes comprehensive documentation of Active Directory through its Open Specifications documentation enabling complete interoperability. In fact, Microsoft initially created this documentation was done under the supervision of the monitoring trustee. This documentation remains complete and accurate, and Microsoft keeps it updated, as required by the terms of the 2004 Decision. Below Microsoft briefly describes how federation works in practice today and details the extensive interoperability enabled for Active Directory as part of Windows Server.

I. Service providers support identity authentication interoperability through federation

As enterprises move to depend on cloud services from multiple vendors (which can include merely using two SaaS applications), they know that they need to deploy IAM solutions that integrate these services together to simplify access for their users. Most enterprises using multiple cloud services deploy some kind of single-sign-on (commonly abbreviated to SSO) solution that relies on federation between services. Single-sign-on allows users to access multiple services without having to sign-in to each one.

Managing identity authentication across multiple services is relevant for any cloud service offering and not only for multiple public cloud offerings. Every cloud service must determine who is trying to access the service ("*authentication*") and which resources each legitimate user should have access to ("*authorization*"). In general, each cloud service provider determines how to manage authentication for its services and most providers rely on their own IAM services to accomplish this. For example, users of Google Workspaces must authenticate to Google's identity system, users of Salesforce must authenticate to Salesforce, and users of Office 365 must authenticate to Microsoft identity system, Entra ID.

Enterprises typically select a single IAM service to serve as the primary directory of users, which the enterprise relies on to perform authentication. Frequently, customers want to authenticate users with their chosen IAM service while allowing those users to access online resources managed by a wholly different provider's IAM service. For example, users might

² Google's response to the Technical Barriers Working Paper published 24 July 2024, para. 3.b.

³ Google's response to the Technical Barriers Working Paper published 24 July 2024, para. 20.

⁴ See European Commission decision of 21 April 2004 in Case COMP/C-3/37.792 – *Microsoft* (the "2004 *Decision*"), in particular Article 5.

authenticate using Google's Cloud Identity IAM service but want access to Microsoft 365 services, which requires using Entra ID. In these scenarios, it is common for enterprises to use *"federation*" between the different IAM services⁵ and every major cloud service for enterprises, including Microsoft's, supports this approach. Federation is a way to have one IAM service entrust authenticating users to another IAM service.

Despite Google's claims, enterprises have a choice in selecting the IAM service to use as their primary directory, including services from Google and Microsoft, even when they want to control access to resources managed by Microsoft Entra ID. For example, Okta works with Entra ID in various ways to manage and enable access to Microsoft applications. ⁶ Okta publishes detailed information on how it uses extensibility points to integrate with Entra ID to enable Okta to be the identity provider for Microsoft services. ⁷ Okta claims that, because of this integration, its offerings provide its customers with "*unique functionality for automation and user experience that leads to long term operational cost savings*," and that, for example, "*[m] ore complex Office 365 environments are significantly simpler to deploy with Okta*."⁸

Google appears to suggest that enterprises must use Entra ID as their primary directory if they want to use Microsoft services because provisioning between Microsoft Entra ID and Google Cloud using the Google Cloud/G Suite Connector written by Microsoft only works one way.⁹ This is wrong. Microsoft wrote this connector to support the scenario where a customer wishes to use Entra ID to sync to and provision users in Google's IAM service in order to also access Google cloud resources. But enterprises who wish to make Google's IAM service the primary directory can provision users into Entra ID using Google's automated user provisioning solution for this purpose.¹⁰ Just like Microsoft, Google also wrote its own connector to allow provisioning of users from its IAM service into Entra ID and Entra ID includes capabilities to enable this scenario.

II. Microsoft publishes comprehensive documentation of Active Directory that enables third-party integrations

Microsoft is committed to ensuring that third-party software can interoperate with Active Directory. Google's claim that "*Microsoft does not provide the necessary interoperability information for third-party cloud IAM solutions to integrate effectively with Active Directory*" is plainly wrong.¹¹ Microsoft has published comprehensive documentation of the Active Directory protocols through its Open Specifications documentation for over fifteen years, and these documents are frequently updated to ensure they remain accurate and up to date.¹² In

⁵ See Technical Barriers Working Paper, paras. 6.27.

⁶ See Microsoft Integrations (<u>https://www.okta.com/partners/microsoft/</u>).

⁷ See Integrate Azure Active Directory with Okta (<u>https://help.okta.com/oie/en-us/content/topics/provisioning/azure/azure-integrate-main.htm</u>).

⁸ See Office 365 – Deploy 6X Faster with Okta (<u>https://www.okta.com/partners/microsoft</u>).

⁹ Federate Google Cloud with Microsoft Entra ID (formerly Azure AD).

¹⁰ Configure Microsoft Office 365 auto-provisioning.

¹¹ Google's response to the Technical Barriers Working Paper published 24 July 2024, para. 20.

¹² The Active Directory protocols are specified in various documents, including [MS-ADTS]: Active Directory Technical Specification, [MS-ADOD]: Active Directory Protocols Overview, and others.

fact, Microsoft is required to provide this documentation under the 2004 Decision, which also applied to the UK as an EU Member State at the time and continues to apply today.¹³ The documentation was created and structured under the supervision of the European Commission's own Monitoring Trustee and remains completely up-to-date and accurate.

Multiple IAM service providers support comprehensive integration with Microsoft Active Directory. For example, Okta explains that its on-demand IAM service "offers the most complete, most reliable and easiest-to-use Active Directory Integration."¹⁴ Similarly, JumpCloud provides Active Directory Integration that it claims is "an alternative to Microsoft's prescribed path" and that also integrates with Google Workspace "making both services better together."¹⁵ The claim that Microsoft is withholding interoperability information about Active Directory in Windows Server and that this forces customers to take Windows Server workloads to Azure is plainly incorrect.

III. Conclusion

In summary, while Microsoft agrees with the CMA that integrating cloud services from multiple vendors, including working with multiple public clouds or deploying hybrid configurations, necessarily has an overhead, the reality is that enterprises already deal with this scenario and the solutions to interoperating amongst multiple IAM services are well understood and operate effectively today. Google's assertion that Microsoft "*unnecessarily and deliberately*" raises costs for customers is wrong.¹⁶

Given the technical nature of and intricacies of some of the submissions made throughout the CMA's investigation, particularly in relation to interoperability, Microsoft believes it is vital for the CMA to have the necessary detail and full context to ensure that it is able to properly assess the evidence it is being provided. As noted above, Microsoft would be pleased to discuss IAM in more detail if the CMA has any remaining questions or concerns as they review the evidence provided by parties to date.

Yours sincerely,

REDACTED

REDACTED Latham & Watkins

¹³ Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as endorsed by leaders at a special meeting of the European Council on 13 December 2019, Article 95(1).

¹⁴ See Okta's Active Directory Integration.

¹⁵ See <u>Active Directory Integration: What is ADI?</u>.

¹⁶ Google's response to the Technical Barriers Working Paper published 24 July 2024, para. 20.