



COMPETITION COMMISSION OF INDIA

Case No. 03 of 2024

In Re:

XYZ

Informant

And

Microsoft Corporation

...Opposite Party No. 1

One Microsoft Way, Redmond, Washington 98052,
United States of America.

Microsoft Corporation (India) Private Limited

...Opposite Party No. 2

T-10 and T-11 3rd Floor, Malik Buildcon Plaza 1, Plot No. 2,
Pocket -6, Sector 12, Dwarka, New Delhi – 110007.

CORAM

Ms. Ravneet Kaur

Chairperson

Mr. Anil Agrawal

Member

Ms. Sweta Kakkad

Member

Mr. Deepak Anurag

Member

Order under Section 26(2) of the Competition Act, 2002

1. The present Information has been filed by XYZ (**Informant**) under Section 19(1)(a) of the Competition Act, 2002 (**Act**), against Microsoft Corporation (**Opposite Party 1 /OP-**



- 1) and Microsoft Corporation (India) Private Limited (**Opposite Party 2 /OP-2**), collectively referred to as Microsoft, *inter alia* alleging contravention of the provisions of Section 4 of the Act. The Informant has sought confidentiality over his identity in the Information.
2. It has been stated in the Information that OP-1 is the world's largest and leading developer of personal-computer software systems and applications and is best known for its software products, including Microsoft Windows Operating Systems (**Windows OS**), the Microsoft Office suite, etc. OP-2 is an Indian subsidiary of OP-1.
 3. It has been submitted by the Informant that since 2015, when Microsoft released its Windows 10 OS edition, it was bundled with pre-installed antivirus software, Microsoft Defender. If any Original Equipment Manufacturer (**OEM**) wants to manufacture a Windows OS-based product, they must mandatorily bundle it with Microsoft Defender.
 4. The Informant stated that starting with Windows 10, separate commercial arrangements to pre-install and pre-activate third-party antivirus software are no longer possible. As only one default antivirus app is allowed on Windows devices, third-party developers may get their software pre-installed through agreements but cannot have it pre-activated. Being set as the default is essential for an antivirus program's functionality, including performing automated background system scans—a core feature distinguishing antivirus software. Without default status, third-party apps lack access to critical features like real-time protection, on-demand scanning, and automatic updates, which are only available to the default antivirus app. Consequently, third-party antivirus apps may struggle to compete effectively and could face elimination from devices due to their inability to function optimally.
 5. The Informant identified three key challenges faced by third-party antivirus developers in competing with Microsoft's bundled antivirus software, Microsoft Defender:
 - a) Antimalware application programming interface (API) Access: Third-party developers must sign the Antimalware API License and Listing Agreement to access



Microsoft's Antimalware API, which allows compatibility with Windows OS. However, this agreement imposes compliance obligations on competitors without offering protective guarantees, rendering it one-sided and potentially anti-competitive.

- b) **Entry into Windows OS:** Competitors can only enter Windows OS via the Microsoft Store, sideloading, or OEM agreements. Entry through the Microsoft Store requires joining the Microsoft Virus Initiative (MVI) program, while sideloading is a complex process with multiple user security warnings. OEM agreements enable pre-installation but not default activation since Microsoft Defender comes pre-installed and pre-activated.
 - c) **Functionality:** Smooth operation of antivirus software on Windows OS requires features such as real-time protection, background scanning, update notifications, and subscription renewal alerts, all of which are restricted to the default antivirus app, leaving third-party apps at a disadvantage.
6. The Informant submitted that even third-party antivirus developers compliant with Microsoft's Antimalware API License and Listing Agreement must join the MVI program to operate effectively on Windows OS. The MVI program is ostensibly designed to align third-party security solutions with Microsoft's technology and strategy. However, membership is conditional upon fulfilling several requirements, including signing a non-disclosure agreement (**NDA**), entering into the Antimalware API License and Listing Agreement, and submitting their software for periodic testing and performance review by Microsoft. The program requires developers to disclose substantial commercial and proprietary technological information, which is then allegedly exploited by Microsoft under the guise of ensuring security and compatibility. While MVI members gain certain advantages not available to non-members, they also relinquish significant control and competitive information, leaving them vulnerable to Microsoft's commercial strategies.
7. The Informant further alleged that Microsoft gains extensive telemetry and app usage data from MVI members, providing it with access to sensitive information on devices running Windows OS. Microsoft decides what data is shared with partners and allegedly uses this



सत्यमेव जयते



data to commercially exploit competitor applications. By analysing the success factors of popular competitor apps, Microsoft integrates those features into its bundled Microsoft Defender, thereby enhancing its own product and ensuring third-party antivirus software cannot effectively compete. This dynamic creates a significant disincentive for antivirus developers to join MVI, as it compromises their competitive position and proprietary information.

8. The Informant also submitted that non-MVI members face significant restrictions in accessing Windows OS, as they cannot use pre-installation or the Microsoft Store and are limited to user-initiated sideloading, which is hampered by disproportionate warnings and, in some cases, outright installation blocks by Microsoft. OEMs avoid pre-installing non-MVI antivirus apps due to their inability to function smoothly under Microsoft's restrictions. Additionally, Microsoft provides non-MVI developers with only a one-week notice for OS updates, making it nearly impossible to ensure timely compatibility. These limitations render third-party antivirus software commercially unviable without MVI membership, effectively forcing developers to join the program to gain access, compatibility, and visibility in the Microsoft Store.
9. For the purpose of the present matter, the Informant has submitted that relevant markets should be considered as the '*market for Licensable Operating Systems (OSs) for desktops in India*' and the '*market for Computer security (antivirus) software for Windows OS in India*'. The Informant has further asserted that Microsoft enjoys a dominant position in the relevant market for Licensable Operating Systems (OSs) for desktops in India and in the market for Computer security (antivirus) software for Windows OS in India. It has been averred that a substantial majority of desktop manufacturers in India utilize the Windows OS, which accounts for approximately 70% of the market share in the country, thereby establishing Microsoft's monopoly in the market for licensable operating systems for desktops in India. Additionally, the Informant has asserted that Microsoft Defender, being pre-installed on all devices operating on Windows OS manufactured post its launch, is presumed to possess a significant market share. By virtue of its pre-installation on 100% of Windows OS devices, Microsoft Defender is alleged to have an absolute monopoly in the market for computer security (antivirus) software for Windows OS in India.



10. Based on the above, the Informant has alleged that Microsoft is abusing its dominant position in the aforementioned markets through the following conduct:

10.1 Microsoft has excluded potentially more efficient competing antivirus software vendors in India by preinstalling and setting Microsoft Defender as the pre activated default antivirus app in Windows OS, thereby violating Section 4(2)(a)(i) of the Act.

10.2 Microsoft has illegally hindered the development and market access of rival security software developers by tying and bundling its own security software, Microsoft Defender with Windows Operating System, thereby violating Section 4(2)(b)(ii) and Section 4(2)(c) of the Act.

10.3 Microsoft has illegally hindered the development and denied market access of rival security software developers by making membership of MVI compulsory in order to get listed in the Microsoft Store and work smoothly in Windows OS, thereby violating Section 4(2)(c) of the Act.

10.4 Microsoft is leveraging its dominance in the market for desktop operating system to protect its position in the market for security software/antivirus software developers in India, thereby violating Section 4(2) (e) of the Act.

11. The Informant has *inter alia* prayed to the Commission to direct Microsoft to cease the anti-competitive practice of bundling Microsoft Security Essentials with its desktop operating system and to ensure fair access for competing antivirus software developers by allowing their participation in the MVI program and making their antivirus solutions available to Windows desktop users.

Consideration by the Commission

12. The Commission considered the Information in its ordinary meeting held on 24.04.2024 and decided to forward a copy of the non-confidential version of the Information to the OPs to seek a response from them and, the Informant was also allowed to file its rejoinder, if any, to such reply of OPs. While Microsoft submitted its reply, no rejoinder was filed by the Informant. Subsequently, the Commission sought additional information and



clarifications from Microsoft, which have since been received. The Commission considered the Information available on record including responses filed by Microsoft, in its ordinary meeting held on 08.01.2025 and decided to pass an appropriate order in due course.

Submissions of Microsoft:

13. Before adverting to the issues arising out of the present Information, it would be appropriate to note, in brief, the submissions of Microsoft in its responses:

13.1 Microsoft Defender's integration within the Windows OS aligns with industry practices and ensures all users are protected at all times against evolving cyber threats. Additionally, the competitive landscape for OS and antivirus solutions is dynamic and robust, featuring multiple significant players and continuous innovation.

13.2 Microsoft Defender is not marketed or sold as a separate product; rather, it is an inherent part of the Windows OS. It is provided at no additional cost to users who purchase the Windows OS.

13.3 Microsoft Defender is one option for Windows users. If a user installs a different third-party antivirus solution that registers itself with Windows (through the MVI) as an application providing real-time protection, Microsoft Defender will automatically be disabled and no longer provide real-time protection. If a third-party antivirus solution reports that it is no longer protecting the user with up-to-date real time protection, then Microsoft Defender will automatically activate.

13.4 The MVI is a program designed to help and collaborate with antivirus vendors to improve the detection and remediation of malware on the Windows OS. The MVI program is optional, and developers of antivirus apps may choose to voluntarily register for it. In the event that users want to choose a third-party antivirus app that is not part of the MVI program, users can easily install and use the alternative antivirus app on Windows OS that can run in parallel with Microsoft Defender.

13.5 OEMs are allowed to pre-install alternative third-party antivirus software on desktops and laptops running Windows OS. The pre-installed antivirus must be of high quality to ensure adequate user protection, and MVI membership serves as a reliable indicator of the software's quality.



13.6. The MVI program enables developers to access specific cybersecurity APIs, allowing their applications to register with Windows as providers of real-time protection. When activated, these applications disable Microsoft Defender automatically, ensuring seamless user experience. To prevent misuse, Microsoft manages API access through the MVI program, safeguarding against malicious applications that could disable Defender and compromise systems. The program ensures transparency by consistently applying and publishing membership criteria. Additionally, MVI offers developers technical resources, tools, prerelease Windows access, and testing programs to meet security standards. Importantly, third-party applications maintain control over their commercial features, including user notifications for subscription renewals.

13.7 Microsoft cannot and does not extract technologically privileged information from other antivirus programs, even if they are part of the MVI program. The only information Microsoft can access is publicly available data that anyone can obtain by downloading the app.

Analysis

14. The grievances of the Informant primarily relate to alleged abuse of dominant position by OPs by way of bundling and tying its antivirus product in Windows OS, thereby violating various provisions of Section 4 of the Act. For examining the allegations pertaining to the alleged abusive conduct of Microsoft under Section 4 of the Act, delineation of the relevant market and determination of the dominance of Microsoft, if any, in those markets is essential.

Determination of Relevant Market and Dominance of Microsoft

15. As stated above, the Informant has proposed relevant markets as the '*market for Licensable Operating Systems (OSs) for desktops in India*' and the '*market for Computer security (antivirus) software for Windows OS in India*'. Microsoft in its submission has argued that Informant's narrower market definition fails to capture the full scope of the competitive environment and the technological advancements that have diversified the market. Additionally, in terms of restricting the relevant market by 'device', the Informant's narrow market analysis incorrectly draws conclusions that Personal



Computers (PCs) require functionalities that are designed specifically for PCs and smartphones require functionalities specific to smart mobile devices. The issue must be considered from the perspective of antivirus software developers and they have been creating solutions that are compatible with various OS and devices. Accordingly, the relevant market in the present case should be defined as *the market for provision of OS on which antivirus solutions can be installed*.

16. At the outset, the Commission notes that OP's delineation of the relevant market as '*market for provision of OS on which antivirus solutions can be installed*' is too broad and inconsistent as it includes the market of OS for all devices including PC, smartphone and tablets. Whereas owing to technological differences and differences in intended usage and characteristics, there is no substitutability amongst smart mobile OS, laptop, and desktop OS, and they form part of separate relevant markets. This is consistent with the Commission's position in the *XYZ (Confidential) and Others Vs. Alphabet Inc. and Others*, where the Commission held that owing to technological differences and differences in intended usage and characteristics, there is no substitutability between smart mobile OS and desktop OS, and they form part of separate relevant markets.
17. The Commission also observes that desktop and laptop operating systems can be divided into two categories: licensable and non-licensable. Licensable operating systems are those that the developer or owner makes available for use by others, either for free or for a licensing fee. Examples include Microsoft Windows and Linux. On the other hand, non-licensable operating systems, such as Apple's macOS, are not offered for licensing by their owners and, therefore, cannot be used by third-party manufacturers such as Dell or HP. Since non-licensable operating systems are not available to third-party device makers, they do not compete in the same market as licensable operating systems. Taking into consideration these features and the different parameters cited *supra*, the Commission delineates the first relevant product market as '*market for Licensable Operating Systems (OSs) for desktops/laptops*.'
18. As regards the geographic market, the Commission notes that since conditions for competition are homogenous in India, the geographic area of India has to be taken as the



relevant geographic market for the purposes of assessment. Accordingly, the first relevant market would be the *‘market for Licensable Operating Systems (OSs) for desktops/laptops in India’*.

19. The Informant has alleged that Microsoft is dominant in this market and has leveraged such dominance to take advantage in another market i.e. *‘market for Computer security (antivirus) software for Windows OS in India’*.
20. The Commission notes that Computer security software, commonly called antivirus software, is designed to prevent, detect, and eliminate malware threats such as viruses, worms, spyware, and ransomware from computers, networks, and IT systems. It offers features such as automatic updates, email scanning, and protection against various malicious activities. While firewalls are essential for regulating network traffic and preventing unauthorized access, they are not substitutes for antivirus software, which focuses on internal system protection. Thus antivirus software constitutes a distinct product market.
21. Further, the Commission also observes that operating system compatibility is crucial for antivirus software developers, as incompatibility can result in poor functionality or inadequate protection against cyber threats, leaving devices and data vulnerable. Compatibility ensures that antivirus software is tailored to work effectively with specific operating systems, such as Windows, macOS, or Linux. Developers optimize their programs by employing distinct scanning techniques and algorithms suited to the unique characteristics of each operating system, enhancing their ability to detect and mitigate threats efficiently. This specialization is essential for maximizing the effectiveness of antivirus solutions in safeguarding system security. Thus, the Commission delineates the second relevant market for assessing the allegations of the Informant as *‘market for desktop/laptop security (antivirus) software for Windows OS in India’*.
22. After delineation of the relevant market(s), the next step would be to determine the dominance of Microsoft in the same. Microsoft argued in its submission that Informant has incorrectly assumed Microsoft’s dominance in the incorrectly defined relevant market



सत्यमेव जयते



of licensable OS for desktops based on market share data alone. It is important to note that market shares alone do not conclusively establish dominance, especially in dynamic markets where competition is robust, and market shares fluctuate. In fact, Windows' overall OS market share in India is only 13.41% whereas Android's market share is as high as 75.78%. The Commission notes that the market share data provided above by Microsoft is in the context of much broader market segments which also include smart phone and tablets in addition to desktops/laptops.

23. The Commission notes from Microsoft's submission dated 10.12.2024 that the company's Windows OS holds an average market share of 70% in the licensable operating systems (OS) market for desktops and laptops in India, based on page views, during the calendar years 2021–2024. Additionally, the top five PC manufacturers in India—HP Inc., Dell Technologies, Lenovo, Acer Group, and Asus—rely on the licensable Windows OS and collectively account for 85% of the market share. Furthermore, Microsoft's significant presence across various segments of the computer system value chain, including operating systems, productivity software (e.g., Word, Excel, PowerPoint, and Outlook), hardware (such as Surface devices and Xbox consoles), and cloud services, provides it with a considerable advantage in the market. Therefore, based on market share, dependence of consumers, and vertical integration of the enterprise, the Commission *prima facie* finds Microsoft to be dominant in the first relevant market i.e. 'market for *Licensable Operating Systems (OSs) for desktops/laptops in India*'.

Assessment of alleged abusive conduct

24. Based on the averments contained in the Information the Commission has identified four issues for determination. The issues and corresponding analysis of the Commission thereon are as under:

Issue 1. Does the inclusion of Microsoft Defender with the Windows operating system constitute an imposition of an unfair condition by Microsoft, thereby violating Section 4(2)(a)(i) of the Act?



25. As per the submissions of the Informant, a user who does not wish to install the Microsoft Security Essentials but only Microsoft Windows does not have the option to do so. By bundling and establishing it as the pre-installed, pre-activated default software, Microsoft appears to shield Microsoft Defender from effective competition from third-party antivirus software vendors and limits capital investment and technical advancements in the antivirus software market.
26. The Commission observes from Microsoft's submissions that there is no compulsion on users to exclusively use Microsoft Defender as their antivirus solution. Users are free to install any third-party antivirus software of their choice, either through the internet or *via* the Microsoft Store. They can opt to continue using Microsoft Defender or replace it with a non-Microsoft solution on Windows. For antivirus applications that do not register with Windows through MVI, these can run in parallel with Microsoft Defender. However, if a user installs a third-party antivirus solution that registers itself with Windows through MVI as providing real-time protection, Microsoft Defender will automatically disable its real-time protection functionality.
27. The Commission further notes that OEMs are also permitted to pre-install alternative third-party antivirus software on desktops and laptops running Windows OS. Additionally, other OS providers, such as macOS and ChromeOS, also include built-in antivirus functionality in place. Therefore, in the absence of an element of compulsion or imposition, *prima facie* there appears to be no violation of Section 4(2)(a)(i) of the Act.

Issue 2. Has Microsoft's conduct resulted in an impediment to technical and scientific development in the market for antivirus applications, thereby violating Section 4(2)(b)(ii) of the Act?

28. The Informant has submitted that Microsoft has illegally hindered the development and market access of rival security software developers by tying and bundling its own security software, Microsoft Defender with the Windows Operating System, thereby violating Section 4(2)(b)(ii) of the Act.



सत्यमेव जयते



29. The Commission notes that the Informant has not provided any evidence to substantiate that there has been any actual or potential impediment to technical and scientific development on account of Microsoft's practices. Additionally, the Commission observes that there are many developers of antivirus software, and each of these providers routinely introduce new features and enhance their offerings to provide better services to customers. This ongoing innovation in the sector indicates that Microsoft's inclusion of Defender has not stifled technological advancement or deterred competition. Moreover, the submissions made by Microsoft further reinforce this view, as they indicate that other operating system providers are also consistently developing and rolling out new security features, updates, and performance enhancements. This suggests that technological progress in the cybersecurity and OS sectors remains dynamic and is not hindered by alleged Microsoft practices. Furthermore, the Commission also notes from the submissions of Microsoft that it neither extracts nor has access to any technologically privileged information from other antivirus programs, including those participating in the MVI program. Thus, allegations against Microsoft in respect of any actual or potential impediment to technical and scientific development appear to be largely speculative and lack relevant proof of harm, and *prima facie* there appears to be no violation of Section 4(2)(b)(ii) of the Act.

Issue-3 Does Microsoft's conduct of bundling its own security software, Microsoft Defender, with the Windows Operating System violate Section 4(2)(d) of the Act?

30. As regards the allegation under Section 4(2)(d) of the Act, the Commission observes that economic literature, as well as the past decision of the Commission (Case No. 15 of 2020: *Harshita Chawla vs Whatsapp and Anr*), has laid down certain conditions which need to be fulfilled to conclude a case of tying. Such conditions are (i) the tying and tied products are two separate products; (ii) the entity concerned is dominant in the market for the tying product; (iii) the customers or consumer does not have a choice to obtain the tying product only without the tied product; and (iv) the tying is capable of restricting/foreclosing competition in the market.



31. The Commission notes that Microsoft submitted that Microsoft Defender is not a separate product but a core security feature integrated into the Windows OS to provide real-time protection against threats like viruses, malware, spyware, and ransomware. This integration ensures that all Windows users receive built-in security. Microsoft also emphasized that Defender is not marketed or sold separately but is inherently included in the OS at no additional cost to users who purchase Windows OS. Additionally, Microsoft contended that it is not dominant in the relevant market. It argued that there is no element of coercion forcing Windows users to rely on Microsoft Defender as their primary or sole antivirus protection. Users remain free to choose and install third-party security solutions. Furthermore, Microsoft asserted that there is no foreclosure in the antivirus market, as several large and well-established cybersecurity vendors continue to operate and compete effectively.
32. The Commission does not agree with Microsoft's integrative approach, which suggests that Microsoft Defender is merely a core security feature of Windows OS. The Commission highlights that there are independent manufacturers specializing in the development of antivirus software, indicating a separate consumer demand and, therefore, a distinct market for antivirus solutions. Furthermore, the Commission has already determined *prima facie* that Microsoft holds a dominant position in the '*market for computer security (antivirus) software for Windows OS in India*'. Given this, the first two conditions for anti-competitive tying—(i) the existence of two separate products and (ii) dominance in the tying product market (Windows OS) appear to be met in this case.
33. On the third condition, i.e. whether there is any compulsion/coercion on the users to necessarily purchase/use the tied product to use the tying product, the Commission observes that Microsoft has submitted that there has been no anti-competitive tying in the present case as there is no element of 'coercion' for the two products to be purchased or used together. According to Microsoft, users retain the autonomy to install and use any antivirus application of their preference, either by downloading it from the internet or by accessing it through the Microsoft Store. This implies that users are not restricted to using Microsoft's built-in security software and can opt for alternative solutions from third-party providers. Furthermore, Microsoft has submitted that various other antivirus applications



सत्यमेव जयते



are pre-installed by OEMs on certain devices. These pre-installed applications are available for immediate use by consumers, offering them additional choices without requiring any additional effort on their part. Thus, the third condition does not appear to be fulfilled.

34. Lastly, as regards the fourth condition, i.e. the actual or likely impact of installation on competition in the market for tied products, the Commission observes that there is no indication of market foreclosure in the antivirus solutions sector. Despite the presence of Microsoft's built-in security software, multiple well-established and prominent players continue to operate in the market without significant barriers to entry or exclusion. Notably, leading cybersecurity firms such as Symantec, Bitdefender, Norton, McAfee, and AVG have remained active in the market since the introduction of Windows 10. Their sustained presence suggests that they have not been driven out or significantly weakened due to Microsoft's practices. Moreover, these companies appear to be competing vigorously, offering a variety of antivirus solutions to consumers. Accordingly, the fourth condition also does not appear to be met either.
35. For the foregoing reasons, the Commission is of the view that the allegation of the Informant under Section 4(2)(d) of the Act is not made out.

Issue 4: Has Microsoft leveraged its dominant position in the market for operating systems for personal computers in India to safeguard its position in the market for computer security (antivirus) software for Windows OS, thereby violating Section 4(2)(e) of the Act?

36. The Commission notes that for a charge of leveraging to sustain, there must be evidence of an active restriction or conditionality imposed, rather than merely providing a product or service for use. In the present case, there is no indication that Microsoft has placed any restrictions or mandatory conditions on users regarding the use of Microsoft Defender. Consumers have the freedom to install and use third-party antivirus applications of their preference, without any technical or contractual barriers preventing them from doing so. Additionally, the cybersecurity market remains highly competitive, with several



सत्यमेव जयते



established players actively operating and offering a range of antivirus solutions. Therefore, in the absence of compelling evidence of restrictive practices, the allegation that Microsoft has leveraged its dominance in the operating system market to protect its position in the computer security software market, in violation of Section 4(2)(e) of the Act, does not appear to be substantiated.

Issue 5: Has Microsoft restricted the development and market access of rival security software developers by making MVI membership a mandatory requirement for listing in the Microsoft Store thereby violating Section 4(2)(c) of the Act?

37. The Informant has alleged that Microsoft has illegally hindered the development of and denied market access to rival security software developers by making membership of MVI compulsory in order to get listed in the Microsoft Store and work smoothly in Windows OS, thereby violating Section 4(2)(c) of the Act.
38. Microsoft in its submissions has stated that the purpose of the MVI program is to assist organizations in enhancing their security solutions on Windows by providing tools, resources, and knowledge to develop reliable and compatible security applications. The program grants access to specific cybersecurity APIs, enabling developers to register their applications for real-time protection and prevent malicious actors from disabling Microsoft Defender. However, MVI membership is not mandatory, as developers can create antivirus applications independently. Microsoft emphasizes that the program is a facilitative measure rather than a gatekeeping mechanism, ensuring high-security standards through consistently applied and transparently communicated criteria. Additionally, MVI members benefit from access to technical resources, prerelease Windows versions, antivirus development tools, and certification programs to maintain compliance with security standards.
39. The Commission observed that non-MVI antivirus developers are not restricted from distributing their applications on Windows, as they can do so through the Microsoft Store and direct downloads from their websites. While non-MVI applications cannot automatically disable Microsoft Defender, they can operate concurrently, and the claim



सत्यमेव जयते



that non-MVI members are blocked is inaccurate. Instead, such applications undergo enhanced scrutiny to ensure that only legitimate software interacts with Microsoft Defender while maintaining user protection. Furthermore, non-MVI applications can notify users of updates and offer their services without obstruction. As noted in the OP's submission, the MVI program is designed to support organizations in improving their security solutions on Windows by providing necessary tools, resources, and knowledge to develop effective, reliable, and compatible products. Thus, Microsoft may pursue its legitimate interest by prescribing certain reasonable compatibility requirements and thereby not appear to be in violation of Section 4(2)(c) of the Act.

40. The Commission notes that in response to the Informant's claim regarding Kaspersky Lab's antitrust complaints filed in 2016 with Russia's Federal Antimonopoly Service and in 2017 with the European Commission and the German Federal Cartel Office, alleging that Microsoft leveraged Windows 10 to promote its own antivirus software over third-party alternatives, Microsoft stated that it reached a settlement agreement with Kaspersky in 2017. Microsoft further clarified that the settlement had a global impact, leading to changes in Windows that were also implemented in versions released in India and remain available to users in the country.
41. Based on the aforesaid, the Commission does not find alleged contravention of the provisions of Section 4 of the Act against Microsoft being made out. In view of the foregoing, the Commission is of the opinion that there exists no *prima facie* case of contravention and the information filed is directed to be closed under Section 26(2) of the Act.
42. Before parting with the order, the Commission deems it appropriate to address the requests for confidentiality filed by parties under Regulation 35 of the General Regulations, 2009 (as amended). The Informant has sought confidentiality over its identity and certain documents/information submitted in the proceedings. Similarly, Microsoft has requested confidentiality concerning specific documents, data, and information filed by them. Considering the grounds put forth by the parties for the grant of confidential treatment, the Commission grants confidentiality to such documents/ information in terms of



सत्यमेव जयते



Regulation 36 of the General Regulations read with Section 57 of the Act for a period of three years from the passing of this order. The Commission also grants confidentiality on the identity of the Informant as prayed. It is, however, made clear that nothing used in this order shall be deemed to be confidential or deemed to have been granted confidentiality as the same has been used for the purposes of the Act in terms of the provisions contained in Section 57 thereof.

43. The Secretary is directed to inform the parties accordingly.

Sd/-
(Ravneet Kaur)
Chairperson

Sd/-
(Anil Agrawal)
Member

Sd/-
(Sweta Kakkad)
Member

Sd/-
(Deepak Anurag)
Member

Date:03/03/2025

New Delhi