UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA
450 Fifth Street NW
Washington, DC 20530

Plaintiff,

v.

KEYSIGHT TECHNOLOGIES, INC.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403; and

SPIRENT COMMUNICATIONS PLC
180 High Street
Crawley, West Sussex RH10 1BD
United Kingdom

Defendants.

COMPLAINT

Keysight Technologies, Inc. ("Keysight") and Spirent Communications plc ("Spirent") are two of the largest global providers of three key types of communications testing and measurement equipment – high speed ethernet testing, network security testing, and radio frequency ("RF") channel emulators – and are significant direct competitors in the United States. Keysight's proposed acquisition of Spirent threatens to substantially lessen competition and harm customers in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18. It should be enjoined to avoid harm to competition.

I. NATURE OF THE ACTION

1. Communications networks connect the world, moving significant volumes of data around the clock. Keysight and Spirent provide critical, highly-specialized equipment used to test various components of communications networks and measure and validate network performance. Network equipment manufacturers, communications network operators, and large cloud computing providers purchase and use this specialized testing equipment to ensure their products and networks operate effectively and securely under normal conditions, and to prepare them to withstand the real-world strain of interruptions, cyberattacks, interference, and high user demand. Because communications technologies are rapidly evolving, the communications industry invests millions of dollars annually in researching, developing, and implementing upgrades to their products to keep pace with technological advancement.

2. Together, Keysight and Spirent dominate three testing and measurement markets in the United States: high-speed ethernet testing, network security testing, and RF channel emulators. Keysight and Spirent are each other's closest competitors in these markets. For years, competition between them has resulted in each company offering discounts, maintaining valuable aftermarket support services, and investing in new and advanced products and features—all to the benefit of their customers and the broader public. Keysight's proposed acquisition of Spirent would eliminate this competition, leading to higher prices; lower quality products, support, and service; and less innovation.

II. DEFENDANTS AND THE PROPOSED TRANSACTION

3. Keysight is a Delaware corporation with its headquarters in Santa Rosa, California. It reported $4.979 billion in global revenues in 2024, $1.769 billion of which were from the United States. Keysight's Communications Solutions Group produces and sells the

products in the relevant markets at issue. The Communications Solutions Group includes two main areas: (i) commercial communications and (ii) aerospace, defense and government.

4. Spirent is a United Kingdom corporation headquartered in Crawley, England, with offices in Calabasas, California and other locations in and outside the United States. It earned $460 million in global revenues in 2024, $257 million of which were from the United States.

5. On March 28, 2024, Keysight offered to purchase Spirent for $1.5 billion. Spirent's board recommended that Spirent shareholders accept Keysight's offer, which they did on May 22, 2024.

III. JURISDICTION AND VENUE

6. The United States brings this action pursuant to Section 15 of the Clayton Act, as amended, 15 U.S.C. § 25, to prevent and restrain Keysight and Spirent from violating Section 7 of the Clayton Act, 15 U.S.C. § 18.

7. Both Keysight and Spirent are corporations that transact business within this District through, among other things, their sales of communications testing and measurement products.

8. Defendants Keysight and Spirent are engaged in a regular, continuous, and substantial flow of interstate commerce and their sales have a substantial effect on interstate commerce, including within this District. The Court has subject-matter jurisdiction pursuant to Section 15 of the Clayton Act, as amended, 15 U.S.C. § 25, and 28 U.S.C. §§ 1331, 1337(a), and 1345.

9. Defendants Keysight and Spirent have consented to venue and personal jurisdiction in this district. Venue is proper in this district under Section 12 of the Clayton Act, 15 U.S.C. § 22 and 28 U.S.C. § 1391.

IV. BACKGROUND

10. Communications networks link together different entities and devices, referred to as "endpoints," to enable the exchange of information between them. Communications networks include computer networks in a large enterprise organization; telecommunications networks that power mobile phones; satellite networks that enable GPS-enabled devices; and cloud-computing networks that store and transmit vast quantities of data. These endpoints can be connected via hardwire (e.g., optical fiber/copper) or wirelessly using radio spectrum. Today, a complex system of interconnected and separate networks allow consumers to store, access, and move data across the world.

11. The communications industry uses specialized testing equipment to verify the performance of communications networks and the devices connected to them. This testing is essential to validate that a network performs as expected, even under non-ideal conditions, such as conditions that interfere with a wireless signal, or to ensure that networks and equipment can handle increasing loads of traffic. Testing also helps ensure that user data is securely protected against the threat of cyberattack. To complete this testing, equipment manufacturers and network operators purchase specialized hardware and software equipment, and they rely on periodic software updates and multi-year services contracts to provide regular maintenance and system upgrades.

12. High-speed ethernet testing, network security testing, and RF channel emulators are used in a lab environment to test network elements before they are deployed in the field. Lab

testing equipment is complex, costly, and relatively fixed. By contrast, equipment used to test networks and devices already in operation – known as live testing equipment – is generally more portable and less expensive than lab testing equipment.

13. Customers use lab testing equipment throughout the lifecycle of a network, even after the network or devices in it have been deployed. Lab testing ensures that communications networks can support updated devices, comply with revised industry standards, and maintain data security as the cybersecurity landscape changes.

14. Lab testing equipment requires constant engineering investment. Network technology changes rapidly: data moves faster, mobile wireless providers deploy new spectrum and new wireless technologies, would-be hackers develop new lines of attack, and device manufacturers make each iteration of their product more sophisticated. Lab testing equipment providers, including Keysight and Spirent, spend millions of dollars each year on research and development to ensure their products keep pace with market changes and employ hundreds of specialized experts dedicated to improving their testing equipment and responding to customer requests.

15. Accurate lab testing capabilities are critical to the development, validation, and maintenance of wireline and wireless communications devices and networks. A wide range of customers depend on specialized lab testing equipment to successfully deploy their networks and devices, including network equipment manufacturers, network operators, chipset manufacturers, "hyperscalers" that offer cloud computing services, research labs, government testing centers, and large companies operating secure internal networks. Equipment cannot be effectively deployed in these complex networks without such testing.

V. RELEVANT MARKETS

16. Each of the three product markets identified below constitutes a line of commerce as that term is used in Section 7 of the Clayton Act, 15 U.S.C. § 18, and each is a relevant product market in which competitive effects can be assessed. The geographic market for each relevant product market is comprised of sales to customers within the United States.

A. High-Speed Ethernet Testing Equipment

17. High-speed ethernet testing equipment tests the performance of both the hardware and software components of high-speed wireline communications networks. Specifically, it tests the functionality of communications both within a given network and across different networks. This testing ensures that wireline networks can support high-bandwidth use cases, such as running artificial intelligence algorithms. These testing products are crucial to ensure that large network operators can support data usage at scale.

18. Customers using high-speed ethernet testing equipment have no reasonable alternatives for testing their wireline network equipment. Solutions developed in-house or relying on open-source software would not provide an adequate alternative for most customers. Attempting to use such options would require costly investments in engineering and other technical resources, can take years to develop, and would not be as reliable or robust as the high-speed ethernet testing equipment available from Keysight or Spirent.

19. A hypothetical monopolist could profitably impose a small but significant and non-transitory price increase for, or otherwise degrade quality of, high-speed ethernet testing equipment customers in the United States. A degradation of quality could entail any dimension of competition, including service, capacity investment, choice of product variety or features, or innovation. Accordingly, high-speed ethernet testing equipment sold to U.S. customers

constitutes a relevant market and line of commerce under Section 7 of the Clayton Act, 15 U.S.C. § 18.

B. Network Security Testing Equipment

20. Network security testing equipment assesses the cybersecurity of wireline networks through laboratory simulation of attacks, testing firewalls as well as other security-related features like proxy and secure content gateways. These products simulate real-world conditions, such as high traffic volumes, to ensure that a network's security policies protect it from attack without impacting performance.

21. Customers that purchase network security testing equipment have no reasonable alternatives. Although some companies make use of open-source software or internally developed tools for limited purposes, self-supply is not a viable option for most customers due to the high costs involved. Customers rely on network security testing equipment to ensure sensitive data are protected from cyberattacks, and they are thus unlikely to rely on unproven and untested solutions in the ordinary course of business.

22. A hypothetical monopolist could profitably impose a small but significant and non-transitory price increase for, or otherwise degrade the quality of, network security testing equipment offered to customers in the United States. A quality degradation could entail any dimension of competition, including service, capacity investment, choice of product variety or features, or innovation. Accordingly, network security testing equipment sold to U.S. customers constitutes a relevant market and line of commerce under Section 7 of the Clayton Act, 15 U.S.C. § 18.

C. RF Channel Emulators

23. RF channel emulators evaluate how wireless networks and devices will react when deployed in the real world, where a wireless signal may not be perfect. Wireless networks transmit data using radio frequency spectrum. Wireless communication networks are used across multiple important industries, including cellular networks, satellite networks, and radar and navigation systems. Unlike in a wireline environment, signal transmission through radio frequency can be subject to substantial interference from weather, large objects, topographical features, and the presence of other competing radio signals.

24. RF channel emulators, also known as "faders," are used in a lab setting. They test whether wireless receivers, such as cell phones or radar handsets, can effectively receive and decode RF signals. A channel emulator adds various impairments to the intended communication path to simulate real-world challenges, such as dense urban settings, mountainous regions, or long distances. This performance testing enables engineers to adjust and optimize designs in a controlled environment to ensure wireless networks perform as expected once they are deployed.

25. Customers that purchase RF channel emulators have no reasonable alternatives. Although some companies make use of open-source software or internally developed tools for limited purposes, self-supply is not a viable option for most customers due to the high costs and technical expertise required to develop internal solutions. Customers rely on RF channel emulators to ensure networks will operate effectively in real-world conditions.

26. A hypothetical monopolist could profitably impose a small but significant and non-transitory price increase for, or otherwise degrade the quality of, RF channel emulators sold to customers in the United States. A degradation of quality could entail any dimension of competition, including quality, service, capacity investment, choice of product variety or

features, or innovation. Accordingly, RF channel emulators sold to U.S. customers constitutes a relevant market and line of commerce under Section 7 of the Clayton Act, 15 U.S.C. § 18.

VI. ANTICOMPETITIVE EFFECTS

27. Keysight and Spirent are the dominant providers of high-speed ethernet testing equipment, network security testing equipment, and RF channel emulators in the United States. Their proposed merger would extinguish the competition between them and would presumptively result in a substantial lessening of competition in each market.

28. The transaction would substantially lessen competition in the market for high-speed ethernet testing equipment in the United States. Keysight and Spirent are the two principal suppliers of high-speed ethernet testing equipment in the United States and have remained the market leaders in this area for many years. In the United States, Keysight and Spirent have a combined market share of approximately 85%. The market for high-speed ethernet testing equipment is already highly concentrated and would become significantly more concentrated as a result of the proposed merger.

29. Keysight and Spirent compete directly against one another to provide high-speed ethernet testing equipment to customers. The handful of other market participants serve far fewer customers and offer much less robust technical solutions than Defendants do. Customers have benefited from competition between Defendants through lower prices, higher quality services, and more robust innovation – an essential feature as technology and network hardware testing components continuously evolve to meet and enable customer innovations.

30. The transaction also would substantially lessen competition in the market for network security testing equipment in the United States. Keysight and Spirent are the two largest suppliers of network security testing equipment in the United States and have remained the

market leaders in this market for many years. In this market, each Defendant earns more than double the revenue of any other competitor; together, Keysight and Spirent would have a combined market share of at least 60% in the United States. The market for network security testing equipment is already highly concentrated and would become significantly more concentrated after the proposed merger.

31. Keysight and Spirent compete head-to-head to provide network security testing equipment to customers. This competition has resulted in lower prices, higher-quality services, and faster product improvements. These updates are essential to keep pace as cybersecurity attackers develop increasingly more sophisticated methods of accessing secure networks.

32. The transaction also would substantially lessen competition in the market for RF channel emulators in the United States. Keysight and Spirent are two of the leading providers of RF channel emulators in the United States, with a combined market share of more than 50%. The market for RF channel emulators is already highly concentrated and would become significantly more concentrated after the proposed merger.

33. Keysight and Spirent compete head-to-head to provide RF channel emulators to customers. This competition has resulted in lower prices, higher-quality services, and robust product improvements. These updates are essential to keep pace as technology improves and wireless networks are used for increasingly more data traffic.

34. Keysight and Spirent are especially close competitors for customers who use RF channel emulators to test terrestrial wireless networks (as opposed to satellite networks) and for customers who need "external" hardware-based faders able to test a full array of RF channel emulation capabilities. Other providers of RF channel emulators only support satellite networks and/or only emulate simple interference with "internal" software-based products. Keysight and

Spirent are the only providers in the United States of RF channel emulators capable of supporting the full array of test environments for terrestrial wireless networks. For U.S. customers that require these capabilities, Keysight and Spirent are the only options.

VII. ABSENCE OF COUNTERVAILING FACTORS

35. It is unlikely that any firm would enter the relevant markets in a timely manner sufficient to prevent the proposed transaction's anticompetitive effects. Successful entry into these specialized markets is difficult, time-consuming, and costly.

36. A prospective entrant would need to invest significant time and capital to design and develop testing products comparable to the Defendants' product lines. In each of the relevant markets, Keysight and Spirent have spent millions of dollars and many years acquiring, building, and refining their products. Moreover, the underlying communications technologies are governed by evolving standards, requiring substantial ongoing investment to ensure that a new product functions effectively with new features and meets new standards. Finally, given that these products impact the performance, security, and reliability of networks that handle sensitive data, a prospective entrant would need to devote significant resources to demonstrate its ability to provide a high-quality product and high-quality service and support, including regular updates. Purchasers of high-speed ethernet lab testing equipment, network security testing equipment, and RF channel emulators have complex needs and are reluctant to rely on any company without an established brand and reputation.

37. Defendants cannot demonstrate verifiable, merger-specific efficiencies sufficient to offset the proposed merger's anticompetitive effects.

VIII. VIOLATIONS ALLEGED

38. Keysight's proposed acquisition of Spirent will eliminate competition between them and would substantially lessen competition in three critical communications testing and measurement equipment markets in the United States in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18.

39. Among other things, the transaction would:

i. eliminate competition between Keysight and Spirent;

ii. likely cause prices of critical communications testing and measurement equipment to be higher than they would be otherwise; and

iii. likely reduce quality, service, choice, and innovation.

IX. REQUEST FOR RELIEF

40. The United States requests:

i. that Keysight's proposed acquisition of Spirent be adjudged to violate Section 7 of the Clayton Act, 15 U.S.C. § 18;

ii. that the Defendants be permanently enjoined and restrained from carrying out the proposed acquisition of Spirent by Keysight or any other transaction that would combine the two companies;

iii. that the United States be awarded costs of this action; and

iv. that the United States be awarded such other relief as the Court may deem just and proper.

Dated: June 2, 2025

Respectfully Submitted,

FOR PLAINTIFF UNITED STATES OF AMERICA:

ABIGAIL A. SLATER (D.C. Bar #90027189)
Assistant Attorney General

ROGER P. ALFORD (D.C. Bar #445158)
Principal Deputy Assistant Attorney General

WILLIAM J. RINNER (D.C. Bar #997485)
Deputy Assistant Attorney General

RYAN DANKS
Director of Civil Enforcement

GEORGE C. NIERLICH (D.C. Bar #1004528)
Deputy Director of Civil Enforcement

JARED A. HUGHES
CORY BRADER LEUCHTEN
Assistant Chiefs, Media, Entertainment, and Communications Section

/s/ Carl Willner
CARL WILLNER* (D.C. Bar #412841)
CARMEL ARIKAT (D.C. Bar #1018208)
KATHERINE CLEMONS (D.C. Bar #1014137)
CURTIS STRONG (D.C. Bar #1005093)
ISABEL AGNEW
Attorneys

U.S. Department of Justice
Antitrust Division
Media, Entertainment, and Communications Section
450 Fifth Street NW, Suite 7000
Washington, DC 20530
Tel.: 202-514-5813
Fax: 202-514-6381
Email: carl.willner@usdoj.gov

*LEAD ATTORNEY TO BE NOTICED