UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,
United States Department of Justice
Antitrust Division
450 Fifth Street NW, Suite 7100
Washington, DC 20530,

Plaintiff,

v.

THALES S.A.
Tour Carpe Diem
31 Place des Corolles – CS 20001
92098 Paris La Defense Cedex
France,

and

GEMALTO N.V.
Barbara Strozzilaan 382
Amsterdam, The Netherlands
1083 HN

Defendants.

Case No.:

COMPLAINT

The United States of America, acting under the direction of the Attorney General of the United States, brings this civil action to enjoin the acquisition of Gemalto N.V. (Gemalto) by Thales S.A. (Thales) and to obtain other equitable relief. The United States alleges as follows:

I. NATURE OF THE ACTION

1. Thales intends to acquire all of the outstanding ordinary shares of Gemalto for approximately $5.64 billion. Thales and Gemalto are the world's leading providers of general

purpose (GP) hardware security modules (HSMs) and are significant direct competitors in the United States.

2. Organizations, including corporations and governmental agencies, use GP HSMs to protect their most sensitive data. GP HSMs are hardened, tamper-resistant hardware devices that strengthen data security by, among other things, making encryption key generation and management, data encryption and decryption, and digital signature creation and verification more secure. GP HSMs are used to achieve higher levels of data security and to meet or exceed established and emerging industry and regulatory standards for cybersecurity.

3. Together, Thales and Gemalto dominate the U.S. market for GP HSMs and face limited competition from a few, much smaller rivals. Thales and Gemalto are each other's closest competitors. They compete head-to-head in the development, marketing, service, and sale of GP HSMs. Thales' proposed acquisition of Gemalto would eliminate this competition, resulting in higher prices; lower quality products, support, and service; and reduced innovation.

4. Accordingly, the transaction is likely to substantially lessen competition in the provision of GP HSMs in the United States, in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18, and should be enjoined.

II. DEFENDANTS AND THE PROPOSED ACQUISITION

5. Thales is an international company incorporated in France with its principal office in Paris. Thales is active globally in five main industries: (i) aeronautics; (ii) space; (iii) ground transportation; (iv) defense; and (v) security. In 2017, it had global revenue of approximately $19.6 billion, operations in fifty-six countries, and approximately 65,100 employees. Thales eSecurity is a business unit of Thales. Thales eSecurity primarily encompasses three legal entities: (1) Thales eSecurity Inc. (based in the United States with offices in Plantation, Florida; San Jose, California; and Boston, Massachusetts), (2) Thales UK Ltd. (based in the United

Kingdom), and (3) Thales Transport & Security HK Ltd. (based in Hong Kong). Thales eSecurity specializes in developing, marketing, and selling data security products including but not limited to GP HSMs, payment HSMs, and encryption and key management software and hardware. Thales sells GP HSMs to customers worldwide, including government and commercial organizations throughout the United States, under the brand name nShield. In 2008, Thales acquired nCipher, a company that specialized in cryptographic security and sold, among other things, GP HSMs under the brand name nCipher. After that acquisition, Thales changed the brand name of those GP HSMs to nShield.

6. Pursuant to its commitments to the European Commission, entered into on November 7, 2018, Thales has agreed to divest its nShield business. As part of these commitments, Thales has separated the nShield business and related assets and personnel from the rest of its businesses and appointed a hold separate manager whose responsibility it is to manage the nShield business as a distinct and separate entity from the businesses retained by Thales until the divestiture is completed. This new business unit is operating under the name nCipher Security.

7. Gemalto is an international digital security company incorporated in the Netherlands with its principal office in Amsterdam. Gemalto is active globally in providing authentication and data protection technology, platforms, and services in five main areas: (i) banking and payment; (ii) enterprise and cybersecurity; (iii) government; (iv) mobile; and (v) machine-to-machine Internet of Things. In 2017, Gemalto had global revenue of approximately $3.7 billion, operations in forty-eight countries, and approximately 15,000 employees. Gemalto develops, markets, and sells GP HSMs, as well as other security solutions and services including but not limited to payment HSMs and encryption and key management

software and hardware. In the United States, Gemalto sells its products and services primarily through SafeNet, Inc. (based in Belcamp, Maryland), SafeNet Assured Technologies, LLC (based in Abingdon, Maryland), and Gemalto Inc. (based in Austin, Texas). Gemalto sells GP HSMs to customers worldwide, including government and commercial organizations throughout the United States, under the brand name SafeNet Luna.

8. On December 17, 2017, Thales and Gemalto entered into an agreement on a recommended all-cash offer by Thales to acquire all of the issued and outstanding ordinary shares of Gemalto for approximately $5.64 billion.

III. JURISDICTION, VENUE, AND INTERSTATE COMMERCE

9. The United States brings this action under Section 15 of the Clayton Act, 15 U.S.C. § 25, to prevent and restrain Defendants from violating Section 7 of the Clayton Act, 15 U.S.C. § 18. This Court has subject-matter jurisdiction over this action under Section 15 of the Clayton Act, 15 U.S.C. § 25, and 28 U.S.C. §§ 1331, 1337(a), and 1345.

10. Defendants market, sell, and service their products, including their GP HSMs, throughout the United States and regularly and continuously transact business and transmit data in connection with these activities in the flow of interstate commerce, which has a substantial effect upon interstate commerce.

11. Defendants consent to personal jurisdiction and venue in this district. This Court has personal jurisdiction over each Defendant and venue is proper under Section 12 of the Clayton Act, 15 U.S.C. § 22, and 28 U.S.C. § 1391(b) and (c).

IV. THE RELEVANT MARKET

A. Industry Background

12. Many U.S. organizations, including commercial enterprises and government agencies, use, transmit, and maintain sensitive electronic data. The universe of sensitive

electronic data has been expanding rapidly and relates to a wide range of subjects, such as personally identifiable information, classified information, health records, financial information, tax records, trade secrets and other confidential business information, software code, and other nonpublic information. Access to this data is often critical to an organization's ability to operate effectively and efficiently. Inappropriate use, theft, corruption, or disclosure of this data could result in significant harm to an organization's customers or constituents and the organization itself.

13. U.S. organizations increasingly rely on encryption as a crucial component of the security measures implemented to safeguard sensitive data from internal and external threats. Encryption is a process that converts readable data (plain text) into an unreadable format (cipher text) using an algorithm and an encryption key. Decryption is the reverse of encryption, converting cipher text back to plain text. Encryption algorithms are based on highly complex math and are often standardized and open source. Encryption keys consist of a randomly generated series of numbers or pairs of randomly generated prime numbers, expressed in bits. Because encryption algorithms are virtually impossible to decipher using today's technology, attackers who want unauthorized access to sensitive data generally focus their efforts on obtaining private encryption keys instead of trying to break the encryption algorithm directly. With the right key, an attacker can freely access an organization's sensitive data. Moreover, a lost or corrupted key could make encrypted data unrecoverable by the organization. Organizations therefore must implement processes and products that create, maintain, protect, and control their encryption keys in a manner that safeguards against improper access or use while simultaneously ensuring the keys are readily available when required for authorized use.

14. GP HSMs provide the most secure way for organizations to effectively manage and protect their encryption keys, and many U.S. organizations use them to protect their most sensitive data. GP HSMs are tamper-resistant hardware environments for secure encryption processing and key management. GP HSMs provide additional security as compared to software-based key management solutions because they are isolated from the host information technology (IT) environment and segregate encryption keys from encrypted data and encryption applications. GP HSMs also enable organizations to implement strong authentication regimes for key management administrators that prevent unauthorized access.

15. GP HSMs are typically independently validated to confirm they provide a level of security specified by various standards. Certifications of compliance with these standards provides assurance to customers that GP HSMs satisfy certain minimum security performance benchmarks. For example, U.S. GP HSM customers frequently rely on the Federal Information Processing Standard (FIPS) 140-2 to assess the level of security provided by a particular GP HSM. FIPS 140-2 is a standard defined by the U.S. National Institute of Standards, which is part of the U.S. Department of Commerce. The standard is mandatory for U.S. government IT security systems that use cryptographic modules to protect sensitive but unclassified information. Commercial enterprises also rely heavily on the standard to assess the security provided by cryptographic modules. FIPS 140-2 comprises four increasing, qualitative levels of security—Levels 1 through 4—for cryptographic modules used to protect sensitive information. Cryptographic modules go through an expensive and time consuming testing process in order to be validated at a particular FIPS 140-2 level. Although software-only modules can be validated under FIPS 140-2, due to increasingly stringent security requirements, organizations must use an

HSM to attain Level 3 security. Thales and Gemalto both provide highly secure GP HSMs that have been validated at FIPS 140-2, Level 3.

16. Thales and Gemalto sell GP HSMs and related services directly to end-user organizations, to resellers who often combine the GP HSMs with additional security products or services, and to cloud service providers (CSPs) who then sell GP HSM services, or HSM-as-a-service (HSMaaS), to their cloud customers. The leading CSPs purchase GP HSMs from third-party suppliers, including Thales and Gemalto.

17. There are, however, many organizations that are reluctant to move their sensitive data to the cloud and use HSMaaS because of security concerns. These organizations continue to rely, to at least some degree, on purchasing and using their own GP HSMs to protect their sensitive data.

18. GP HSMs typically must be integrated into or configured to operate within an organization's existing IT environment. An organization needs assurance that a GP HSM will be an effective component of what may be an already complex data security infrastructure. Because of this, the GP HSM sales process typically includes a comprehensive exchange of information between the potential customer organization and GP HSM supplier.

19. Once an organization has installed a GP HSM into its IT environment and is using it to protect its keys and to provide a secure data encryption environment, any breakdowns or malfunctions in the GP HSM could not only compromise the sensitive data but also jeopardize the organization's ability to perform day-to-day tasks that are necessary for the organization to carry out its business. Post-sales customer support and service are therefore essential conduct carried out by successful GP HSM suppliers. Many customers will not even consider a potential GP HSM supplier who has not established a strong reputation for providing quality GP HSMs

and continuous and effective post-sales service and support. Thales and Gemalto both have strong reputations for high-quality post-sales service and support. Thales and Gemalto provide this service and support to their direct customers and indirectly to other customers by assisting their resellers.

20. Thales and Gemalto both create and maintain confidential price lists for their respective GP HSMs, additional GP HSM components and accessories, and services. Confidential discount rates are then applied to the price list to determine the prices that are applicable to resellers. Thales and Gemalto authorize, customer-by-customer, confidential discounts from the prices on the price list, and in the case of resellers, additional discounts to the discounted prices already available to the reseller. Thales and Gemalto regularly approve significant discounts on GP HSMs when competing against each other.

B. Relevant Market

21. GP HSMs are most frequently included as components of complex encryption solutions used by government and private organizations to safeguard their most sensitive data. Use of GP HSMs is often specified by regulations, industry standards, or an organization's auditors or security policies, or is otherwise deemed necessary to safeguard the organization's most sensitive data or provide the organization's customers or constituents with confidence that their sensitive data will be adequately protected. Organizations that use GP HSMs have determined that less expensive alternatives to GP HSMs, such as software-based key management solutions, provide inadequate security for their most sensitive data. Some organizations will not even use cloud-based GP HSMaaS, and, if they do, will require an on-premises GP HSM to provide an additional layer of encryption security for encryption keys stored in a cloud-based GP HSM. Many customers are unwilling to entrust the protection of their most sensitive data to HSMaaS provided by a CSP. In order to provide HSMaaS to those

customers that are willing to outsource at least some their GP HSM needs, CSPs purchase GP HSMs from the Defendants and the Defendants' GP HSM competitors.

22. Defendants market, sell, and service GP HSMs for use by organizations across the United States. Because GP HSMs are used to protect an organization's most sensitive data, U.S. customers require GP HSM suppliers to possess the demonstrated ability to provide both high-quality GP HSMs and high-quality post-sales service and support in the United States.

23. A hypothetical GP HSM monopolist could profitably impose a small but significant and non-transitory increase in price on GP HSM customers in the United States. Accordingly, GP HSMs sold to U.S. customers is a relevant market for purposes of analyzing the likely competitive effects of the proposed acquisition under Section 7 of the Clayton Act, 15 U.S.C. § 18.

V. ANTICOMPETITIVE EFFECTS OF THE PROPOSED ACQUISITION

24. Together, Thales and Gemalto dominate the GP HSM market in the United States. Thales and Gemalto are the two leading providers of GP HSMs in the United States, with individual market shares of approximately 30% and 36%, respectively, and a combined market share of approximately 66%. Thales' proposed acquisition of Gemalto likely would substantially lessen competition and harm customers in the U.S. GP HSM market by eliminating head-to-head competition between the two leading suppliers in the United States. The acquisition likely would result in higher prices, lower quality, reduced choice, and reduced innovation. Thales' proposed acquisition of Gemalto would substantially increase market concentration in an already highly concentrated market. The proposed acquisition violates Section 7 of the Clayton Act.

25. Thales and Gemalto currently compete head-to-head and their respective GP HSMs are each other's closest substitutes. Thales and Gemalto regularly approve significant discounts on GP HSMs when competing against each other. Competition between the two

companies has also spurred innovation in the past. Thales' proposed acquisition of Gemalto would eliminate this head-to-head competition and reduce innovation, in addition to significantly increasing concentration in a highly concentrated market. As a result, Thales would emerge as the clearly dominant provider of GP HSMs in the United States with the ability to exercise substantial market power, increasing the likelihood that Thales could unilaterally increase prices or reduce its efforts to improve the quality of its products and services.

VI. ABSENCE OF COUNTERVAILING FACTORS

26. It is unlikely that any firm would enter the relevant product and geographic markets alleged herein in a timely manner sufficient to defeat the likely anticompetitive effects of the proposed acquisition. Successful entry in the development, marketing, sale, and service of GP HSMs is difficult, time-consuming, and costly.

27. Any new entrant would be required to expend significant time and capital to design and develop a series of GP HSMs that are at least comparable to Defendants' GP HSM product lines in terms of functionality and ability to interoperate with a wide range of encryption solutions and IT resources. Moreover, a new entrant, as well as any existing GP HSM provider seeking to expand and become a viable competitor in the supply of GP HSMs for use by individual organizations in the United States in on-premises security solutions, would need to spend significant time and effort to demonstrate its ability to provide quality GP HSMs for such use and continuous, high-quality post-sales service in the United States. It is unlikely that any such entry or expansion effort would produce an economically viable alternative to the merged firm in time to counteract the competitive harm likely to result from the proposed transaction.

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

VII. VIOLATION ALLEGED

29. The United States incorporates the allegations of paragraphs 1 through 28 above.

30. The proposed acquisition of Gemalto by Thales is likely to substantially lessen competition for the development and supply of GP HSMs in the United States in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18.

31. Unless enjoined, the proposed acquisition likely will have the following anticompetitive effects, among others:

(a) actual and potential competition between Thales and Gemalto in the development, sale, and service of GP HSMs in the United States will be eliminated;

(b) competition in the development, sale, and service of GP HSMs in the United States in general will be substantially lessened;

(c) prices of GP HSMs will increase;

(d) improvements or upgrades to the quality or functionality of GP HSMs will be less frequent and less substantial;

(e) the quality of service for GP HSMs will decline; and

(f) organizations in the United States that require GP HSMs for use in on-premises security solutions will be especially vulnerable to an exercise of market power by the merged firm.

VIII. REQUEST FOR RELIEF

32. The United States requests that this Court:

(a) adjudge and decree that Thales' proposed acquisition of Gemalto would be unlawful and would violate Section 7 of the Clayton Act, 15 U.S.C. § 18;

(b) permanently enjoin and restrain Defendants and all persons acting on their behalf from carrying out the December 17, 2017, agreement on a recommended all-cash

offer by Thales to acquire all of the issued and outstanding ordinary shares of Gemalto, or from entering into or carrying out any other contract, agreement, plan, or understanding, or taking any other action, to combine Thales and Gemalto;

(c) award the United States its costs for this action; and

(d) award the United States such other and further relief as this Court deems just and proper.

Dated: February 26, 2019

Respectfully submitted,

FOR PLAINTIFF UNITED STATES OF AMERICA:

MAKAN DELRAHIM (D.C. Bar # 457795)
Assistant Attorney General for Antitrust

BERNARD A. NIGRO, JR.
(D.C. Bar # 412357)
Deputy Assistant Attorney General

PATRICIA A. BRINK
Director of Civil Enforcement

AARON D. HOAG
Chief, Technology and Financial Services Section

DANIELLE G. HAUCK
ADAM T. SEVERT
Assistant Chiefs, Technology and Financial Services Section

KELLY M. SCHOOLMEESTER
(D.C. Bar # 1008354)
MAUREEN T. CASEY
(D.C. Bar # 415893)
CATHARINE S. WRIGHT
(D.C. Bar # 1019454)
CHINITA M. SINKLER
BINDI R. BHAGAT
CORY BRADER LEUCHTEN
R. CAMERON GOWER
RYAN T. KARR
DAVID J. SHAW
(D.C. Bar # 996525)
AARON COMENETZ
(D.C. Bar # 479572)
KENT BROWN

Attorneys for the United States

United States Department of Justice
Antitrust Division
450 Fifth Street, NW, Suite 7100
Washington, D.C. 20530
Tel.: (202) 598-2693
Fax: (202) 616-8544
Email: kelly.schoolmeester@usdoj.gov