



to do business in Texas with its principal place of business at 9442 Capital of Texas Highway North, Suite 400, Austin, TX 78759. Gemalto can be served via their registered agent Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808.

4. This Court has personal jurisdiction over Gemalto because Gemalto has committed, and continues to commit, acts of infringement in the state of Texas, conducted business in the state of Texas, and/or has engaged in continuous and systematic activities in the state of Texas.

5. This Court has exclusive subject matter jurisdiction pursuant to 28 U.S.C. §1338(a) under the Patent Laws of the United States.

6. Venue is proper in this judicial district and division pursuant to 28 U.S.C. §1400(b) and 28 U.S.C. §1391 (b) because Gemalto has committed acts of infringement within this judicial district and division and Gemalto is subject to personal jurisdiction in this judicial district.

#### **THE PATENT-IN-SUIT**

7. Prior to July 18, 1997, David C. Reardon invented a novel and non-obvious method and system for providing security to computers in compliance with the FIPS 140-2 standards. The method and system relies on an improved, novel and non-obvious use of asynchronous encryption keys, also known as public/private key pairs which may be implemented through the use of a USB “token” to block unauthorized access to a computer memory, and/or to block unauthorized access to various computers that are networked together.

8. In general, non-legal terms, the ‘635 Patent relates to a method and system for providing security for a computer by implementing an additional level of user control over a computer through a security gateway that is positioned upstream of the computer's CPU. The

security gateway functions to block unauthorized access to the CPU which operates programs, and to block access to the peripheral devices that are directed by the CPU to implement programs or retrieve and store data. Because the additional level of security control is independent of the CPU, the invention makes it impossible for any program run by the user to cross over into restricted memory areas to read, alter, or erase data.

9. Reardon applied for and obtained United States Patent No. 6,212,635 entitled “Network Security System Allowing Access and Modification to a Security Subsystem After Initial Installation When a Master Token is in Place” which was duly and legally issued on April 3, 2001 (the ‘635 Patent). A true and correct copy of the ‘635 Patent is attached as Exhibit A.

10. Vortex owns all substantial rights in and to the ‘635 patent.

#### **DEFENDANT’S INFRINGEMENT**

11. In 2001, the National Institute of Standards and Technology published the Federal Information Processing Standards Publication 140-2 (“FIPS 140-2”). This standard involves security requirements for cryptographic modules, which protect sensitive information stored on computers. As will be pointed out in greater detail below, Defendant Gemalto advertises that its StarSign Crypto USB Token is certified as complying with FIPS 140-2 level 3 Certification.

12. Defendant Gemalto manufactures and sells a USB Cryptographic Token called “Gemalto Smart Guardian FIPS Cryptographic Module” (the “Accused Product”).

13. The Accused Product is employed to provide security for computers via a removable USB stick in compliance with the FIPS 140-2 Level 3 Certification Standards.

14. Defendant Gemalto uses the Accused Product at least during the development, internal testing, and maintenance of the Accused Product by having Gemalto employees, or other

entities under Gemalto's control, perform the steps in at least claim 1 of the '635 Patent as illustrated in Exhibit 2.

15. Defendant Gemalto makes, offers to sell and sells the Accused Product for use in practicing the method for providing computer security claimed in at least claim 1 of the '635 Patent in conjunction with a removable USB token.

16. On information and belief, at least one customer of Gemalto uses the Accused Product to perform the steps in at least claim 1 of the '635 Patent as illustrated in Exhibit 2.

17. Vortex has retained the undersigned attorneys and has agreed to pay them a reasonable fee.

### **COUNT I**

#### **DIRECT INFRINGEMENT OF U.S. PATENT NO. 6,212,635**

18. Plaintiff repeats and re-alleges paragraphs 1 through 17 above as fully and completely as if set forth herein verbatim.

19. Claim 1 of the '635 Patent includes a preamble or introductory portion followed by five steps (a) through (e).

20. The preamble of Claim 1 of the '635 Patent states: A method for providing security for a computer comprised of a central processing unit, peripheral and file storage devices, at least one of which can be used as a token access device that can read and write files to removable storage media suitable for use as a token, a computer operating system, and a CPU independent security subsystem which includes a security control unit and programmable auxiliary memory".

21. The Accused Product is used in a method as described in Paragraph 20 hereof via a USB Token removably connected to a computer that includes the ability to read and write files

to removable storage media suitable for use as a USB Token where the computer system includes a security control unit and a programmable auxiliary memory thus corresponding to the preamble of Claim 1 as explained in greater detail on pages 1 – 6 of Exhibit 2.

22. Step (a) of Claim 1 of the ‘635 Patent states: “generating with said security control unit a security subsystem key pair comprised of a public key and a private key;”

23. The Accused Product as used with the security control unit generates a key pair, namely a public key and a private key as described in Paragraph 22 hereof, thus corresponding to Step (a) of Claim 1 of the ‘635 Patent as explained in greater detail on pages 6 -8 of Exhibit 2.

24. Step (b) of Claim 1 of the ‘635 Patent states: “storing said private key data in a memory location which is under the control of the said security subsystem;”

25. The private key data is stored in a memory location that is under the control of the security subsystem and the Accused Product, as described in Paragraph 24 hereof, thus corresponding to Step (b) of Claim 1 of the ‘635 Patent as explained in greater detail on pages 8-9 of Exhibit 2.

26. Step (c) of Claim 1 of the ‘635 Patent states: “creating with said security - subsystem a key file encrypted with said public key and writing the key file to a master token by means of said token access device, such that said encrypted key file can only be decrypted and authenticated by the security subsystem using its corresponding private key;”

27. The Accused Product together with the security subsystem creates the key file encrypted with the public key and writes that key file to a master token via a token access device so that the encrypted key file may only be decrypted and authenticated by the security subsystem using its corresponding private key, as described in Paragraph 26 hereof, thus corresponding to Step (c) of Claim 1 of the ‘635 Patent as explained in greater detail on pages 9-11 of Exhibit 2.

28. Step (d) of Claim 1 of the '635 Patent states: "allowing access to said security subsystem after initial installation and setup by said computer operating system for installation and modification of security requirements only when said master token is placed into an appropriate file storage device and said encrypted key file has been authenticated by the security subsystem;"

29. After initialization or installation, access to the security subsystem is precluded unless the master token is in the proper location and the encrypted file is authenticated by that security subsystem, as described in Paragraph 28 hereof, thus corresponding to Step (d) of Claim 1 of the '635 Patent as explained in greater detail on pages 11-16 of Exhibit 2.

30. Step (e) of Claim 1 of the '635 Patent states: "denying file and peripheral device access requests by the central processing unit when the security requirements are not satisfied."

31. If and when the central processing unit seeks access to files and or peripheral devices, the Accused Product functions to deny access if the security requirements of the method and system are not met, as described in Paragraph 30 hereof, thus corresponding to Step (e) of Claim 1 of the '635 Patent as explained in greater detail on pages 16-17 of Exhibit 2.

32. Since at least 2012, Defendant Gemalto has make, used and sold the Accused Product, the use involving at least testing the Accused Product in accordance with the steps described above in Paragraphs 19-31 hereof.

33. The use of the Accused Product as described in Paragraphs 19-32 hereof infringes at least Claim 1 of the '635 Patent either literally or under the doctrine of equivalents in violation of 35 U.S.C. § 271(a).

34. The activities of Gemalto as set forth in this Count I have been without license, permission or authorization from Plaintiff.

35. The activities of Gemalto as set forth in this Count I have been and continue to be to the injury and detriment of Plaintiff and irreparable harm to Plaintiff.

**WHEREFORE, PLAINTIFF PRAYS:**

- A. For judgment that Gemalto has infringed the '635 Patent;
- B. For an accounting and an award of damages sufficient to compensate Plaintiff for the infringement but in no event less than a reasonable royalty;
- C. For an award of costs; and
- D. For such other and further relief as to the Court may appear just and reasonable.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 26, 2016

Respectfully submitted,

**SCHNEIDER ROTHMAN INTELLECTUAL  
PROPERTY LAW GROUP, LLC**

*/s/ Joel B. Rothman*

---

Joel B. Rothman

Florida Bar Number 98220

[Joel.rothman@sriplaw.com](mailto:Joel.rothman@sriplaw.com)

Jerold I. Schneider

Florida Bar Number 26975

[Jerold.schneider@sriplaw.com](mailto:Jerold.schneider@sriplaw.com)

4651 North Federal Highway

Boca Raton, Florida 33431

561.404.4350 – Telephone

561.404.4353 – Facsimile

**BUETHER JOE & CARPENTER, LLC**

By:

Kenneth P. Kula

State Bar No. 24004749

[Ken.Kula@BJCIPLaw.com](mailto:Ken.Kula@BJCIPLaw.com)

1700 Pacific Avenue

Suite 4750

Dallas, Texas 75201

214.730.5660 – Telephone

972.707.1248 – Facsimile

**ATTORNEYS FOR PLAINTIFF  
VORTEX PATHWAY LLC**