IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SOVERAIN IP, LLC, ***Plaintiff,*** v. **APPLE, INC.** ***Defendant.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Soverain IP, LLC ("Soverain" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,191,447 ("the '447 patent") 8,935,706 ("the '706 patent"); 5,708,780 ("the '780 patent"); and 6,212,634 ("the '634 patent") (collectively, the "patents-in-suit" or the "Soverain Patents"). Defendant Apple, Inc. ("Apple" or "Defendant") infringes each of the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. This case arises from Apple's infringement of Soverain's data extraction and network management patent portfolio. Soverain is the owner by assignment and exclusive licensee to twenty-four issued United States patents, multiple pending patent applications,[1] and numerous foreign patent assets.[2]

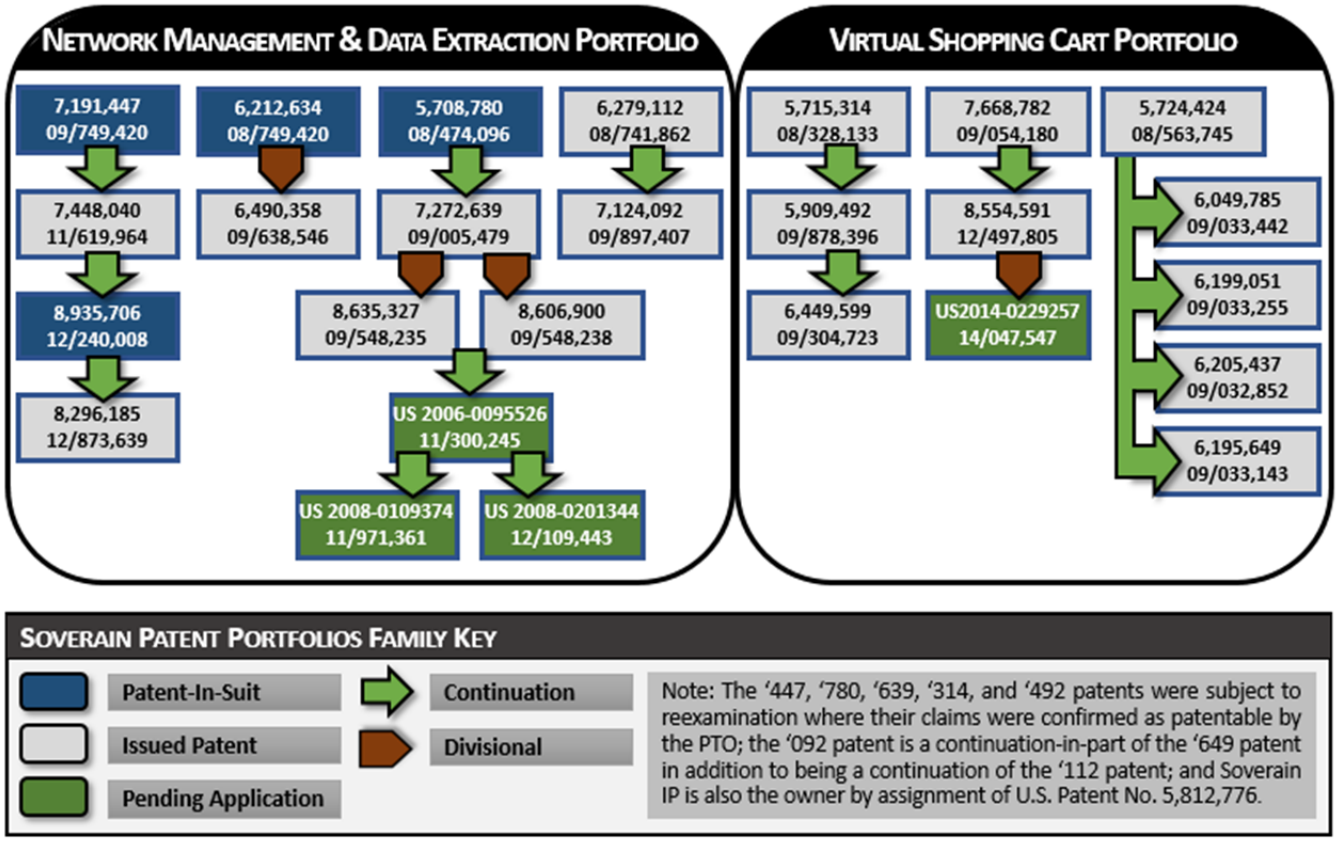
2. The patents asserted in this case arose from the innovative work of Open Market, Inc. ("Open Market"), an innovative tech firm that in 1993 developed groundbreaking technologies for the then-nascent Internet. Open Market was founded at a time when conducting commercial transactions over the Internet was in its beginning stages. Previous uses of the Internet had largely been limited to academic research and military defense work.

[1] *See* U.S. Patent App. Nos. 11/300,245; 11/971,361; 12/109,443; 14/047,547.

[2] *See e.g*., JP 4485548, JP 3762882B2, EP 0803105B1, DE 69633564T2.

3. Professor David K. Gifford of the Massachusetts Institute of Technology, co-founder of Open Market, and inventor of fourteen of the Soverain patents, recognized the potential of enabling secure transactions over computer networks. Professor Gifford and other Open Market employees raced against other companies to bring one of the first secure transaction management systems to market. With the technology developed, Open Market filed for the patents that would comprise the two Soverain Patent Portfolios.

4. Open Market's groundbreaking inventions led to the issuance of patents that comprise two technology portfolios: (1) the virtual shopping cart portfolio and (2) the network management and data extraction portfolio. The below diagram shows Soverain's patents, pending patent applications, and the Soverain patents Apple infringes.



SOVERAIN'S LANDMARK DATA EXTRACTION AND NETWORK TECHNOLOGIES

5. Open Market's flagship Internet transaction product, the Open Market Transact system ("Transact") offered a full suite of software technologies, including content management,

authorization protocols, and customer relationship management. Transact contained functionality for separating the management of transactions from the management of content, allowing companies to securely and centrally manage transactions using content located on multiple distributed Web servers.

6. In 1995, Open Market began commercial shipment of Transact.[3] Transact was quickly embraced by the market, and its early customers included: Novell,[4] Sprint,[5] Disney,[6] AT&T,[7] and Hewlett-Packard.[8] In March of 1996, the New York Times described Open Market's transaction management products as being adopted by Time Warner, Banc One, and First Union.

> Open Market will be competing with Netscape's I-Store and Merchant Server of Microsoft. Besides Time Warner, Open Market has signed several big customers including Banc One, First Union Bank, Hewlett-Packard, Digital Equipment and Bloomberg, the financial publisher. Time Warner has been offering electronic versions of Time, People, Sports Illustrated, Money and other publications free on its Pathfinder Web site.[9]

7. By the late 1990s, Transact was an established market leader in e-commerce

---

[3] Ellis Booker, *Internet Security Boosted*, COMPUTERWORLD at 14 (April 17, 1995) ("Last month, Open Market became the first vendor to release a Web server that supports both SHT'I'P and SSL.").

[4] Jessica Davis, *Novell, Open Market Ink Deal*, INFOWORLD at 6 (March 25, 1996) ("Novell has licensed OM-SecureLink commerce server software for the Internet, and plans to integrate OM-SecureLink with Novell's Web server by the third quarter.").

[5] *Sprint Chooses Open Market's Transact as Key Offering of its E-Commerce Services*, PRESS RELEASE (September 27, 2000) ("Sprint will host Transact and offer its functionality as a service for these enterprise sites.").

[6] Eric Nee, *Surf's Up*, FORBES ONLINE (July 27, 1998), available at: https://www.forbes.com/forbes/1998/0727/6202106a.html ("Today Open Market is a leading supplier of Internet commerce software. More than 1,000 Web sites use Open Market software to transact business. Its clients include Disney, which sells on the Internet everything you can buy in one of its shopping mall stores, and Analog Devices, which allows engineers to find and order examples of integrated circuits on its Web site.").

[7] Jeff Symoens, *Transact 3.0: Scalable Solution*, INFOWORLD at 68 (September 8, 1997) ("AT&T is using Transact as part of SecureBuy, a service that gives merchants the infrastructure to run an electronic store on the internet.").

[8] *HP And Open Market Offer Mission-Critical E-Commerce Services*, HP OPEN MARKET PRESS RELEASE (November 18, 1998) ("Open Market is the first member of HP`s Domain Commerce alliance program to integrate HP`s MC/ServiceGuard with its products.").

[9] Glenn Rifkin, *Open Market Hopes It'll be Next Netscape*, N.Y. TIMES (March 4, 1996).

technology, commanding dominant market share of the transactional software market against companies like Microsoft and IBM.[10]

8. The following collection of news articles shows some of the headlines that Open Market's Transact product garnered in the computer industry press from 1996 to 2000.

Sandy Reed, *First-Ever Review of I-commerce System Right For New Section Debut*, INFOWORLD at 73 (September 8, 1997); Matthew Nelson, *Open Market adds Object Support to I-commerce Product*, INFOWORLD at 58 (February 16, 1998.); Ellen Messmer, *Open Market to Liven Up Web-Based Publishing*, NETWORK WORLD at 16 (November 9, 1998); Mitch Wagner, *Open market Upgrade Will Support Big Business On 'Net*, COMPUTERWORLD at 8 (December 9, 1996); Ellen Messmer, *Open Market to Debut e-Comm Tools*, NETWORK WORLD at 12 (March 27, 2000); Kim Nash, *Open Market Aids Web Site Upkeep*, COMPUTERWORLD at 12 (March 11, 1996).

9. The inventors of the Soverain Patents include Open Market's founders and engineers. The inventors of the Soverain Patents comprise:

[10] Eric Nee, *Surf's Up*, FORBES ONLINE (July 27, 1998); *3 Big New Customers for Open Market, Inc.*, N.Y. TIMES (April 24, 1995) ("Open Market Inc. will announce today that three major media companies will use its software and services to provide content and conduct business on the Internet. A privately held company based in Cambridge, Mass., Open Market said it had signed agreements to provide technology to the Tribune Company, Advance Publications and the Time Inc. unit of Time Warner.").

10. Professor David K. Gifford is a professor of electrical engineering and computer science at the Massachusetts Institute of Technology ("MIT") and co-founder of Open Market. Mr. Gifford has been a member of the MIT faculty since 1982 and leads the Programming Systems Research Group at the MIT Laboratory for Computer Science. Professor Gifford is a named inventor on fourteen of Soverain's issued patents.[11]

11. Professor Gifford is the author of over one hundred journal articles and his research areas focus on programming language development; information discovery, retrieval, and distribution; and computation using biological substrates. Professor Gifford earned his S.B. in 1976 from MIT and his M.S. and Ph.D. in electrical engineering from Stanford.

12. Professor Gifford was elected as a fellow by the Association for Computing Machinery, for "contributions to distributed systems, e-commerce and content distribution."[12]

13. Dr. Lawrence Stewart was Open Market's Chief Technology Officer. Dr. Stewart is the co-inventor of nine of Soverain's patents.[13] Dr. Stewart previously held positions at Xerox Palo Alto Research Center ("PARC") and Digital Equipment Corporation. Recently, when writing about his role as a co-inventor of Soverain's patents, Dr. Stewart described the intellectual effort behind the inventions.

> The relevant source code of the Open Marketplace system as of October 1994 was included with the patent application for anyone to read – over 50 printed pages of code. In other words, ***Open Market showed that these inventions weren't just a theory but an actual working system.*** Open Market submitted the source code to the Patent Office on microfiche since there was no way to submit machine readable appendices back in 1994.[14]

---

[11] *See* U.S. Patent Nos. 4,845,658; 5,812,776; 5,724,424; 6,279,112; 6,205,437; 6,195,649; 6,199,051; 6,049,785; 7,191,447; 7,124,092; 7,448,040; 8,935,706; 8,554,591; and 8,286,185.

[12] *Gifford Named ACM Fellow*, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY NEWS (December 13, 2011), available at: https://www.csail.mit.edu/node/1651.

[13] *See* U.S. Patent Nos. 7,272,639; 6,449,599; 8,635,327; 8,606,900; 8,554,591; 5,715,314; 5,708,780; 5,909,492; and 7,668,782.

[14] Lawrence Steward, *The CAFC Got It Wrong In Soverain v. Newegg*, IPWATCHDOG.COM WEBSITE (December 30, 2013), available at: http://www.ipwatchdog.com/2013/12/30/the-cafc-got-it-wrong/id=47141/ (emphasis added).

Dr. Stewart received an S.B. in Electrical Engineering from MIT in 1976, followed by M.S. and Ph.D. degrees from Stanford University in 1977 and 1981, respectively. Dr. Stewart is also the author (with fellow Soverain patent inventor Winfield Treese) of the computer science textbook, *Designing Systems for Internet Commerce* (Addison-Wesley, 2002).

14. Dr. John R. Ellis was Open Market's Architect and Technical Lead. Dr. Ellis subsequently was the Senior Vice President of Engineering at AltaVista Internet and has held positions at Xerox PARC and Amazon.com. Dr. Ellis is a named inventor of four Soverain patents.[15] Dr. Ellis holds a Ph.D. from Yale University and BSE from Princeton University.

15. Dr. Daniel Earl Geer, Jr. served as Director of, Engineering at Open Market and named inventor of two Soverain Patents.[16] Dr. Geer was the former President of USENIX, the advanced computing systems association and served as Chief Scientist at Verdasys, Inc. and Digital Guardian, Inc. Dr. Geer holds degrees from Harvard University and MIT.

16. Winfield Treese was previously the Associate Director of the Hariri Institute for Computing at Boston University. Mr. Treese served as Open Market's Vice President of Technology where he was responsible for the security architecture of Open Market's products. Mr. Treese is a named inventor of eight Soverain patents.[17] Mr. Treese was the chair of the Transport Layer Security (TLS) Working Group of the Internet Engineering Task Force (IETF), the Internet standard successor to SSL. Mr. Treese also chaired the 8th USENIX Security Symposium. Mr. Treese is the co-author of the book *Designing Systems for Internet Commerce* (Addison-Wesley, 2002).

[15] *See* U.S. Patent Nos. 7,448,040; 8,935,706; 8,286,185; and 7,191,447.

[16] *See* U.S. Patent Nos. 6,490,358 and 6,212,634.

[17] *See* U.S. Patent Nos. 7,448,040; 8,935,706; 8,286,185; 5,708,780; 7,272,639; 8,635,327; 8,606,900; and 7,191,447.

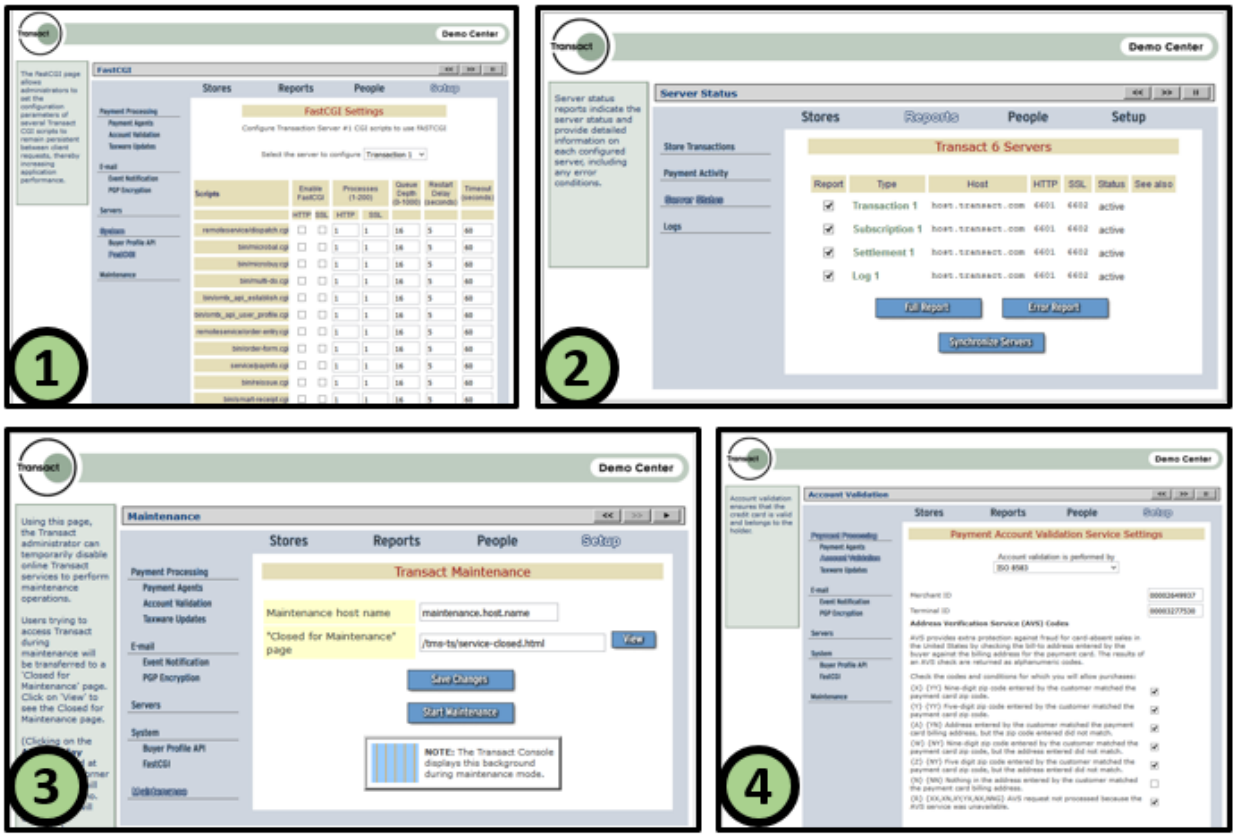
SOVERAIN'S TRANSACT SYSTEM

17. From 1996 through 2000, Open Market's product, Transact, was a leader in the e-commerce field, holding the majority of the global market for transaction management systems.[18] When the first Soverain patents issued in 1998, Open Market was hailed for its "secure, robust, distributed architecture." Jeff Symoens, *Transact 3.0: Scalable Solution*, INFOWORLD at 63 (September 8, 1998). Gary Eichorn, chief executive officer of Open Market, stated that Open Market was selling its "transaction engine to telecommunications companies, banks and Internet service providers. They're then offering commerce services to smaller companies." HOTSEAT: GARY EICHORN, CEO OF OPEN MARKET, DESCRIBES HOW TRANSACTIONS WILL HIT THE WEB, InfoWorld at 47 (March 17, 1997).

18. Transact provided an end-to-end solution for secure transaction management over the Internet. Transact included the following components: (1) a transaction server for managing orders, (2) a subscription server for security and authentication by managing access to digital content, (3) a log server for secure management of log entries, and (4) a settlement server for managing the authorization of transactions. A review of Transact in InfoWorld magazine stated "if you're comfortable with Transact's $125,000 opening price tag, it offers an exceptional architecture and a strong feature set that will handle back-end transaction processing." Jeff Symoens, *Transact 3.0: Scalable Solution*, INFOWORLD at 63 (September 8, 1998).

19. The following images of Soverain's Transact product show: (1) FastCGI configuration screen for keeping application processes running between requests (unlike CGI the system did not require extra overhead by requiring the system start a new process and initializing an application each time a request is made on the system); (2) a server status screen for monitoring the status of multiple hosts running Transact; (3) a maintenance screen for managing system maintenance; and (4) an account validation service setting screen for managing transaction security and authentication.

[18] *Investors Bid Up Internet Stock*, N.Y. TIMES (May 24, 1996) (In May 1996, Open Market made an initial public offering valuing the company at $1.2 billion.).



A COLLECTION OF IMAGES OF THE OPEN MARKET TRANSACTION SYSTEM (the numbered annotations correspond to the (1) FastCGI settings, (2) server status screen, (3) Transact maintenance settings, and (4) account validation settings).

20. As the 2000s approached, larger technology companies entered the transaction management field; the dot-com bubble then burst.[19] As a result, Open Market went through a restructuring and was purchased by Divine interVentures, Inc. ("Divine") for approximately $70 million in 2001.[20] As a result of the purchase, Divine acquired Open Market's patent portfolio and its Transact software product.

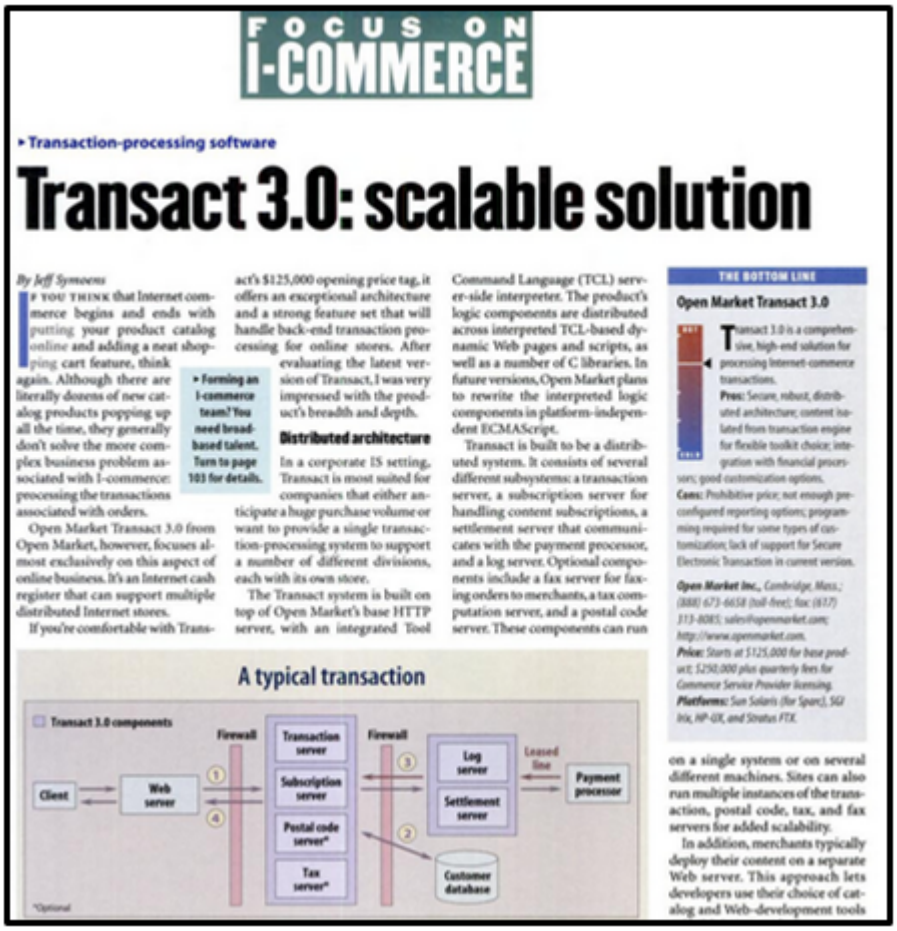
21. Divine was a venture capital investment company founded in May 1999. Divine focused on "professional services, Web-based technology, and managed services." *Id.* At its

[19] *See* Editorial, *The Dot-Com Bubble Bursts*, N.Y. TIMES, Dec. 24, 2000, at WK8 (describing the aftermath of the dot-com bubble bursting).

[20] *Divine to Buy Open Market*, NETWORK WORLD at 8 (August 20, 2001) ("Professional services and software company Divine last week agree to buy struggling Open Market in a stock deal work about $59 million.").

peak, Divine employed approximately 3,000 people in more than 20 locations worldwide and offered approximately 50 software products.

22. In 2003, Transact was acquired by Soverain Software. Soverain Software also acquired the patents from the original Open Market inventors and innovators.



FOCUS ON I-COMMERCE

▸ Transaction-processing software

Transact 3.0: scalable solution

By Jeff Symoens

IF YOU THINK that Internet commerce begins and ends with putting your product catalog online and adding a neat shopping cart feature, think again. Although there are literally dozens of new catalog products popping up all the time, they generally don't solve the more complex business problem associated with I-commerce: processing the transactions associated with orders.

Open Market Transact 3.0 from Open Market, however, focuses almost exclusively on this aspect of online business. It's an Internet cash register that can support multiple distributed Internet stores.

If you're comfortable with Transact's $125,000 opening price tag, it offers an exceptional architecture and a strong feature set that will handle back-end transaction processing for online stores. After evaluating the latest version of Transact, I was very impressed with the product's breadth and depth.

▸ Forming an I-commerce team? You need broad-based talent. Turn to page 103 for details.

Distributed architecture

In a corporate IS setting, Transact is most suited for companies that either anticipate a huge purchase volume or want to provide a single transaction-processing system to support a number of different divisions, each with its own store.

The Transact system is built on top of Open Market's base HTTP server, with an integrated Tool Command Language (TCL) server-side interpreter. The product's logic components are distributed across interpreted TCL-based dynamic Web pages and scripts, as well as a number of C libraries. In future versions, Open Market plans to rewrite the interpreted logic components in platform-independent ECMAScript.

Transact is built to be a distributed system. It consists of several different subsystems: a transaction server, a subscription server for handling content subscriptions, a settlement server that communicates with the payment processor, and a log server. Optional components include a fax server for faxing orders to merchants, a tax computation server, and a postal code server. These components can run on a single system or on several different machines. Sites can also run multiple instances of the transaction, postal code, tax, and fax servers for added scalability.

In addition, merchants typically deploy their content on a separate Web server. This approach lets developers use their choice of catalog and Web-development tools

A typical transaction

THE BOTTOM LINE

Open Market Transact 3.0

Transact 3.0 is a comprehensive, high-end solution for processing Internet-commerce transactions.

Pros: Secure, robust, distributed architecture; content isolated from transaction engine for flexible toolkit choice; integration with financial processors; good customization options.

Cons: Prohibitive price; not enough preconfigured reporting options; programming required for some types of customization; lack of support for Secure Electronic Transaction in current version.

***Open Market Inc.**, Cambridge, Mass.; (888) 673-6658 (toll-free); fax (617) 373-8085; sales@openmarket.com; http://www.openmarket.com.*

***Price:** Starts at $125,000 for base product; $250,000 plus quarterly fees for Commerce Service Provider licensing.*

***Platforms:** Sun Solaris (for Spare), SGI Irix, HP-UX, and Stratus FTX.*

Jeff Symoens, *Transact 3.0: Scalable Solution*, INFOWORLD at 63 (September 8, 1998) ("Transact 3.0 is a comprehensive, high-end solution for processing Internet-commerce transactions. Pros: Secure, robust, distributed architecture.").

SOVERAIN'S PATENT PORTFOLIO

23. Soverain's patents and published patent applications have been cited in over 6,000 issued United States patents and published patent applications as prior art before the United States Patent and Trademark Office.[21] Companies whose patents and patent applications cite the

[21] The over 6,000 forward citations to the Soverain Patents do not include patent applications that were abandoned prior to publication in the face of the Soverain Patents.

Soverain patents include: Microsoft Corporation, Oracle Corporation, Facebook, Inc., AT&T, Inc., International Business Machines Corporation, Dell, Inc., etc.

24. It is difficult today to recall a time before Soverain's patented technology had become part of the platform used to operate many websites. But prior to the mid to late 1990's, when the applications leading to the patents in suit were filed, nothing like the patented functionality had been devised, let alone implemented. The simplicity and intuitive features of the patented technology soon became apparent. Almost overnight, companies abandoned older technologies that often required customers to dial in directly to specific sites, shop for products using function codes or other keypad commands, and fax or phone in orders rather than complete transactions online.

The above images show major Internet properties contemporaneous (and later) to the inventions conceived in the Soverain patents, including: (1) Microsoft.com (August 1995), (2) Amazon.com (July 1995), and (3) Apple.com (July 1997).

25. The Soverain network management and data extraction patent portfolio includes technology that allows companies to streamline and secure the single sign-on process, extract data from hosts over a network, and authenticate and encrypt data using asymmetric keys.

26. Soverain has maintained and developed the Open Market patent portfolio, which now consists of over 50 issued and pending U.S. and international patents covering key aspects of e-commerce technology.

Open Market wins three I-commerce patents

■ Company to pursue licensing fees

By Matthew Nelson and Dylan Tweney

OPEN MARKET has been granted three patents that cover the basic building blocks of Internet-commerce sites.

The patents cover real-time processing of credit- and debit-card payments via the Internet, server-based electronic shopping carts, and digital authentication using URL-based session identifiers.

Open Market said that "many" I-commerce companies are now infringing on the patents, but "our strong preference will be to sell our software or to license the appropriate technology," said Gary Eichhorn, CEO at Open Market.

Companies that may be forced

Chris Stevens, a senior analyst at the Aberdeen Group, in Boston.

I-commerce vendors are not immediately worried about Open Market's claims.

THE WALL STREET JOURNAL.

By **Nick Wingfield** The Wall Street Journal Interactive Edition
Updated March 4, 1998 12:01 a.m. ET

SAN FRANCISCO -- Shares of Internet-software firm Open Market surged 15% on Tuesday following news that it has received several broad-ranging patents related to electronic commerce.

The Burlington, Mass. Company's stock rose 2 3/8 to 18 1/8 on the Nasdaq Stock Market. At one point Tuesday, the stock hit 18 3/8 – a 52-weel high.

Nick Wingfield, *Three Patents Lift Open Market as Observers Guess Their Worth*, WALL ST. J., Mar. 4, 1998 (reporting that one analyst stated: "The most important thing is that it will allow them to be acknowledged as a leader and be sought after for strategic relationships"); Matthew Nelson and Dylan Tweney, *Open Market Wins Three I-Commerce Patents*, INFOWORLD at 10 (March 9, 1998).

27. Confirming the value of Soverain patents, licensees have paid millions of dollars for a license to practice the technology taught in the Soverain patents. For example, Amazon.com, Inc. paid 40,000,000 dollars to license the Soverain patents.[22]

THE PARTIES

[22] Thom Weidlich, *Amazon.Com Set to Pay On Patents*, THE SEATTLE TIMES (August 12, 2005) ("Amazon.com, the world's largest Internet retailer, agreed to pay $40 million to Soverain Software to settle two lawsuits over patents related to online shopping.").

SOVERAIN IP, LLC

28. McKinney, Texas based Soverain owns the intellectual property rights to information management solutions that allow companies and individuals to manage Internet content, encrypt network based information, and manage access to network based information.

29. Soverain's principal place of business is located at 6851 Virginia Parkway, Suite 214, McKinney, Texas 75071. Like Defendant Apple, Soverain relies on its intellectual property for its financial viability.[23]

APPLE, INC.

30. On information and belief, Apple is a California corporation with its principal office at 1 Infinite Loop, Cupertino, California, 95014. Apple can be served through its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

31. On information and belief, Apple has offices in Texas where it sells, develops, and/or markets its products including:

- Apple developers integral to the accused products' infringing capabilities.
- Apple's Austin office is currently undergoing a $300 million expansion and growing from 3500 to 7000 employees.[24]
- Apple operated a patent licensing company in Plano, Texas through its majority-owned subsidiary Rockstar Consortium.
- The supplier of numerous Apple chips (via Samsung) is located in or near the Eastern District of Texas.

32. According to Apple's website, Apple offers infringing products for sale throughout the United States and Canada, including in the Eastern District of Texas. Further, Apple advertises its infringing products throughout the Eastern District of Texas and claims

---

[23] John Paczkowski, *Apple COO [Tim Cook]: "Will Not Stand For Having Our IP Ripped Off*, ALLTHINGSDIGITAL.COM, January 21, 2009 (We will not stand for having our IP ripped off, and we will use every weapon at our disposal.").

[24] Nicole Raney, *Apple Continues Massive Austin Expansion With New Acquisition*, AUSTINCULTUREMAP.COM, April 27, 2015, http://austin.culturemap.com/news/innovation/04-27-15-apple-expansion-offices-lease-southwest-austin-jobs/ ("The massive operations center and satellite office spaces are an extension of Apple's headquarters in Cupertino, California. In addition to providing overflow space for Apple's main hub, Austin houses Apple's hardware development and support teams.").

financial benefits through its conducting of business in Texas, including: (1) accepting monies from the state of Texas relating to Apple's engagements with Texas entities;[25] (2) ongoing contracts with the state of Texas;[26] (3) Apple's agreement to be subject to the laws and jurisdiction of Texas;[27] (4) Apple's certification that it is licensed to conduct business in Texas;[28] (5) Apple's assent to Texas insurance liability;[29] and (6) Apple's agreement (in prior contracts with the state of Texas) to make documentation available to residents of Texas.[30]

33. On information and belief, Apple has asserted its patents in federal courts, including the Eastern District of Texas.[31] And, Apple has acquired companies relevant to the accused products, including Intrinsity, Inc., which is based in Texas.

---

[25] *Apple in Texas: State of Texas Purchase Agreement(s)*, APPLE WEBSITE, September 2015, http://www.apple.com/education/purchase/contracts/states/tx.html; *Texas Department of Information Resources: Apple Inc. Contract Overview*, TEXAS GOVERNMENT WEBSITE, September 2015, http://dir.texas.gov/View-Search/Contracts-Detail.aspx?contractnumber=DIR-SDD-2068&keyword=apple.

[26] *DIR Contract No. DIR-SDD-2068*, STATE OF TEXAS DEPARTMENT OF INFORMATION RESOURCES CONTRACT FOR PRODUCTS AND RELATED SERVICES ORACLE AMERICA, INC. (2015), http://publishingext.dir.texas.gov/portal/internal/contracts-and-services/Contracts/DIR-SDD-2068%20Contract.pdf.

[27] *Id*. at Appendix A § F ("The laws of the State shall govern the construction and interpretation of the Contract.").

[28] *Id*. at Appendix A § D ("Vendor [Apple] and its Order Fulfiller shall be authorized and validly existing under the laws of its state of organization, and shall be authorized to do business in the State of Texas.").

[29] *Id.* at Appendix A § N ("licensed in the State of Texas, and authorized to provide the corresponding coverage").

[30] *Id.* at Appendix A § V(1) ("Pursuant to S.B. 1368 of the 83rd Texas Legislature, Regular Session, Vendor is required to make any information created or exchanged with the State pursuant to this Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.").

[31] *See Affinity Labs of Tex., LLC v. Apple, Inc.*, 2009 WL 7376918, *4 (E.D. Tex. Aug. 25, 2009) (describing Apple Computer's previous litigation); *Apple Computer, Inc. v. Creative Tech. Ltd. and Creative Labs Inc.*, Case No. 06-cv-149, Dkt. No. 1 (E.D. Tex. Filed July 19, 2006) (asserting infringement of U.S. Patent No. 7,046,230); *see also* Testimony from Apple's Corporate Representative in *VirnetX Inc. v. Apple Inc*., Case No. 6:10-CV-417 (E.D. Tex. filed Aug. 10, 2011), Trial Tr., 11/02/12, 38:18-22; see also *id.* at 37:23-24 ("It's a pretty short flight, so it's not a big deal."). More recently, Apple, as majority owner of the Rockstar Consortium, filed a complaint in this District a year ago. *See Rockstar Consortium v. Google, Inc.*, Case No. 13-CV-893-JRG (E.D. Tex. filed Oct. 31, 2013). Apple filed suit against HTC in the District of

34. Apple's sale and distribution of products and services that infringe the patents-in-suit has caused and continues to cause injury to Soverain.

JURISDICTION AND VENUE

35. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

36. Upon information and belief, this Court has personal jurisdiction over Apple in this action because Apple has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Apple would not offend traditional notions of fair play and substantial justice. Defendant Apple, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Apple is registered to do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

37. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Apple is registered to do business in the State of Texas, has offices in the State of Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

TECHNOLOGY BACKGROUND

U.S. PATENT NO. 7,191,447

38. U.S. Patent No. 7,191,447 ("the '447 patent") entitled, *Managing Transfer of Information in a Communications Network*, was filed on August 25, 2000, and claims priority to

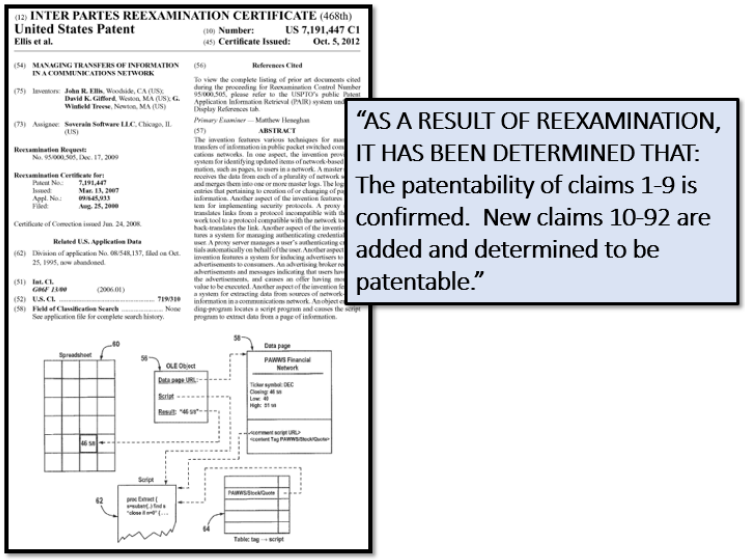
---

Delaware across the continent. *See Apple, Inc. v. HTC, et al.*, 1:10-CV-0167 (D. Del. filed Mar. 2, 2010).

October 25, 1995. The '447 patent is subject to a 35 U.S.C. § 154(b) term extension of 615 days. Soverain is the owner by assignment of the '447 patent. A true and correct copy of the '447 patent is attached hereto as Exhibit A. The '447 patent claims specific methods and systems for managing transfers of information in communications networks such as the World Wide Web.

39. All the claims in the '447 patent were subject to *inter partes* reexamination before the United States Patent Office. The reexamination certificate confirming all claims was issued on October 5, 2012. In addition to confirming the patentability of all claims of the '447 patent, 83 additional claims were added and determined to be patentable over multiple references that were not cited during the prosecution of the '447 patent.

40. During the reexamination proceeding, the United States Patent and Trademark Office Board of Patent Appeals and Interferences confirmed the patentability of the claims over four references.[32]



Reexam Ctrl. No. 95/000,505, '447 PATENT, CERT. ISSUED, OCTOBER 5, 2012.

41. The '447 patent teaches various techniques for managing transfers of information in public packet switched communications networks. For example, the '447 patent teaches a system where a server receives data from one or more networked servers and merges the data

[32] *Decision of the United States Patent and Trademark Office Board of Appeals and Interferences*, *INTER PARTES* REEXAMINATION CONTROL NO. 95/000,505 (January 26, 2012).

into one or more master logs. The ‘447 patent also teaches a system for implementing security protocols wherein a proxy server translates links between an incompatible network protocol to a compatible network protocol and then back-translates the link. The ‘447 patent also discloses a system for extracting data from sources of network-based information in a communication network using an object embedding program that locates a script program and causes the script program to extract data and make it available over a computer network.

42. The ‘447 patent and its underlying application, foreign counterparts, and its related patents have been cited by 135 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘447 patent family as relevant prior art:

- International Business Machines Corporation
- Telefonaktiebolaget L M Ericsson
- Alcatel-Lucent USA, Inc.
- Juniper Networks, Inc.
- Yellowpages.Com LLC
- General Electric Company
- Microsoft Corporation
- Kaspersky Lab Zao
- Lucent Technologies, Inc.
- AOL, Inc.
- Facebook, Inc.
- Siemens Aktiengesellschaft
- Fujitsu Limited
- Vodafone Group plc
- Charles Schwab & Co., Inc.
- Salesforce.com, Inc.
- Samsung Electronics Co., Ltd.
- Amazon.com, Inc.

U.S. PATENT NO. 8,935,706

43. U.S. Patent No. 8,935,706 (“the ’706 patent”) entitled, *Managing Transfers of Information in a Communications Network*, was filed on September 29, 2008, and issued on January 13, 2015. The ‘706 patent is subject to a 35 U.S.C. § 154(b) term extension of 524 days. Soverain is the owner by assignment of the ‘706 patent. A true and correct copy of the ‘706

patent is attached hereto as Exhibit B. The '706 patent claims specific methods and systems for implementing security protocols over a network. The patent teaches the use of server to translate links from a protocol incompatible with an Internet browser to a protocol that is compatible with the same browser. The patent also teaches systems and methods for managing the authentication credentials of a user over a computer network.

44. The '706 patent teaches a system for managing authentication credentials on a public packet switched communications network that includes network servers that receive requests for data that is then transmitted to the requesting party. In one example, a proxy server, maintains a table of authenticating credentials for each network server. The proxy server receives a request for authentication from a network server, retrieves authentication credentials from the table, and transmits the authenticating credentials to the network server. The network server upon receiving the credentials forwards the requested data to the requesting computer.

45. The '706 patent teaches the managing of user authentication credentials using a proxy server. The '706 patent is directed at solving a problem unique to computer networks – centrally managing numerous authentication credentials for computer users. Using the same authenticating credentials for a large number of services increases the risk that a breach in security in connection with one service will affect other services. Moreover, a user may be able to use a particular set of authenticating credentials in connection with one service but not another service, for example if one of the credentials is already being used by another user of the other service. The invention is directed at solving issues relating to having users type in a user ID and password each time a user visits a network service.

46. The '706 patent and its underlying application, foreign counterparts, and related domestic patents and patent applications have been cited by 135 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '706 patent family as relevant prior art:

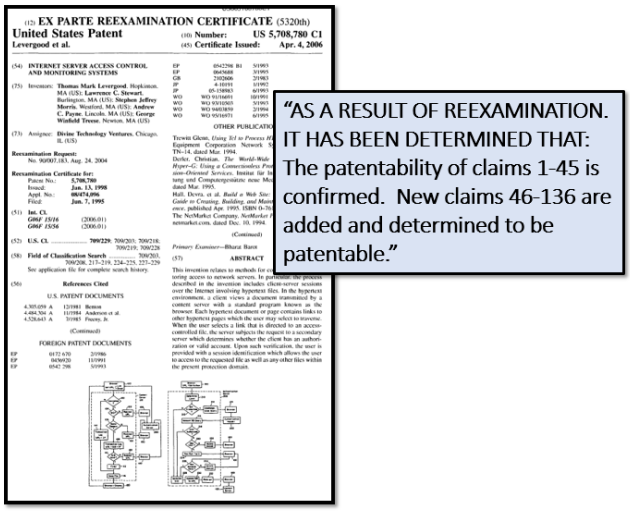
- International Business Machines Corporation
- Telefonaktiebolaget L M Ericsson

- Alcatel-Lucent USA, Inc.
- Juniper Networks, Inc.
- Yellowpages.Com LLC
- General Electric Company
- Microsoft Corporation
- Kaspersky Lab Zao
- Lucent Technologies, Inc.
- AOL, Inc.
- Facebook, Inc.
- Siemens Aktiengesellschaft
- Fujitsu Limited
- Vodafone Group plc
- Charles Schwab & Co., Inc.

U.S. PATENT NO. 5,708,780

47. U.S. Patent No. 5,708,780 ("the '780 patent") entitled, *Internet Server Access Control and Monitoring*, was filed on June 7, 1995, and issued on January 13, 1998. Soverain is the owner by assignment of the '780 patent. A true and correct copy of the '780 patent is attached hereto as Exhibit C. The '780 patent claims specific methods and systems for controlling and monitoring access to network servers. In particular, the process described in the invention includes client-server sessions over the Internet involving hypertext files.

48. The '780 patent was subject to *inter partes* reexamination. The reexamination proceeding culminated with the United States Patent and Trademark Office confirming the patentability of all 45 claims of the '780 patent over 260 prior art references, including over 120 patent references.33



Reexam Ctrl. No. 90/007,183, '780 PATENT, CERT. ISSUED, APRIL 4, 2006.

49. In addition to confirming the patentability of all claims in the ’780 patent, the United States Patent and Trademark Office confirmed the patentability of 90 new claims which were added to the ‘780 patent.

50. The ‘780 patent has been subject to review by Courts in the Eastern District of Texas. In prior orders, the Court denied a motion for partial summary judgment that claims 28 and 32-42 are indefinite under 35 U.S.C. § 112.[34]

51. The ‘780 patent teaches the use a “session identifier” to permit web servers to recognize a series of inquiries (or “service requests”) from the same client during an online session, and to control and monitor the client’s access to information on a website. This technology is important due to the “stateless” nature of the Internet.

52. The ‘780 Patent discloses the use of a web server that assigns a session identifier, which can be as simple as a string of text or numbers, in response to an initial service request from a client. When the server receives a subsequent request with the same session identifier appended to it, the server can then associate that request with earlier requests. The session identifier allows the web server to recognize the client during a series of requests and responses, to provide access to information resources which the user is authorized to access, and to monitor the user’s access.

53. The ‘780 patent discloses the use of a “session identifier” for operating on a “stateless network,” such as the Internet, meaning that the system can simultaneously handle multiple communications from different users. The claimed methods and systems achieve this, in part, by appending a unique “session identifier” to each user request.

---

[33] Reexam Ctrl. Nos. 90/007,183, ‘780 PATENT, CERT. ISSUED, APRIL 4, 2006.

[34] *Soverain Software LLC v. Amazon.com, Inc.*, Case No. 04-cv-00014-LED, Dkt. No. 497 (August 8, 2005).

54. The '780 patent has been the subject of a *Markman* order in the Eastern District of Texas. Specifically, the Court interpreted seventeen disputed terms in the '780 patent. The Court grouped the terms "in groups relating to: (1) path name in a URL, (2) session, (3) hypertext, (4) authentication server, and (5) means-plus-function elements."[35]

55. The means-plus-function claims in the '780 patent have been previously construed by the Court:

> The Court agrees with Soverain that limiting the claims beyond what is disclosed in the block diagrams is not required by case law and penalizes the inventors for submitting software code during prosecution. . . [36]

56. The court went on to identify specific structures for the mean-plus-function elements that corresponded to the means-plus-function elements. The below excerpt from the Court's *Markman* Order shows the means-plus-function elements and the associated structure for two exemplary terms.

DISPUTED CLAIM TERMS	COURT'S CONSTRUCTION
means for servicing service requests from a client which include the session identifier Claim 32	Content server (element 120 in Fig. 2A and element 52 in Fig. 3), executing a computer program implementing algorithm shown in Fig. 2A, including blocks 110, 112, and 116, or the client server exchange 9 and 10 in Fig. 3.
means for providing the session identifier Claim 33	Authentication server (element 200 in Figs. 2A and 2B, element 54 in Fig. 3), executing a computer program implementing algorithm steps as shown in Fig. 2B, including blocks 228, 230, and 232.

Soverain Software LLC v. Amazon, Inc., Case No. 04-cv-00014-LED, Dkt. No. 246 at 24 (April 7, 2005).

57. One or more of the claims of the '780 patent recite a means or step for performing a specified function. The corresponding structure(s) in the '780 patent specification and

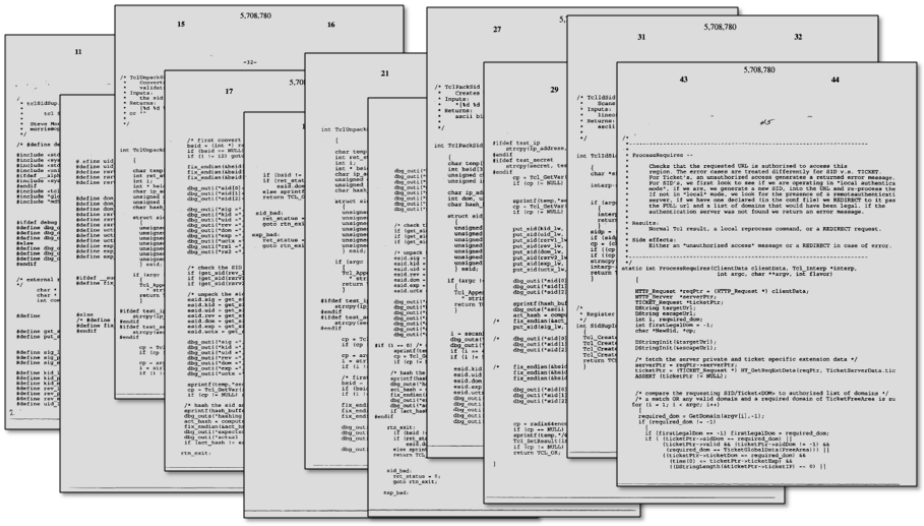
[35] *Soverain Software LLC v. Amazon, Inc.*, Case No. 04-cv-00014-LED, Dkt. No. 246 (April 7, 2005).

[36] *Id.* at 9.

appendix include computer code that improves the functioning of a computer. '780 patent, cols. 11-114.

58. One or more of the claims in the '780 patent recite means-plus-function claim limitations governed by 35 U.S.C. § 112, ¶ 6.

59. The '780 patent discloses computer algorithms in an appendix to the specification. In addition to the structures and algorithms disclosed throughout the specification, these algorithms correspond to means-plus-function claims in the '780 patent.



'780 patent, cols. 11-114 (excerpt of some of the computer algorithms disclosed in an appendix to the specification).

60. Means-plus-function claims such as those included in the '780 patent are inherently not abstract ideas. In *Enfish LLC v. Microsoft Corp*., the Federal Circuit upheld the patentability of claims containing means-plus-function elements. "Accordingly, we find that the claims at issue in this appeal are not directed to an abstract idea within the meaning of Alice. Rather, they are directed to a specific improvement to the way computers operate, embodied in the self-referential table." 822 F.3d 1327, 1336 (Fed. Cir. 2016). Stanford Law Professor Mark Lemley described the basis for means-plus-function elements conferring patentability:

> If the patent is interpreted as a means-plus-function claim, it will be limited to the particular software implementation the patentee actually built or

described. Such a narrow, specific claim should not be an unpatentable "abstract idea."[37]

61. The '780 patent has been cited by 1,840 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '780 patent as relevant prior art.

- International Business Machines Corporation (cited in 61 patents and patent applications)
- Microsoft Corporation (cited in 62 patents and patent applications)
- Oracle Corporation
- Amazon.com, Inc.
- AT&T Corp.
- Cisco Systems, Inc.
- Dell, Inc.
- eBay, Inc.
- First Data Corporation
- Google, Inc.
- Hewlett-Packard Company
- Level 3 Communications, LLC
- Mcaffe, Inc.
- Ricoh Co., Ltd.
- Yahoo!, Inc.
- Xerox Corporation
- NEC Corporation
- Goldman Sachs & Co.
- Facebook, Inc.
- Comcast Corporation
- Intel Corporation
- Akamai Technologies, Inc.

62. The '780 patent relates to methods for controlling and monitoring access to network servers through the use of a session identifier. This session identifier allows web servers to recognize and service multiple requests from the same client and control access to the server without repeated authentication.

U.S. PATENT NO. 6,212,634

63. U.S. Patent No. 6,212,634 ("the '634 patent") entitled, *Certifying Authorization in Computer Networks*, was filed on November 11, 1996, and issued on April 3, 2001. Soverain is the owner by assignment of the '634 patent. A true and correct copy of the '634 patent is attached hereto as Exhibit D. The '634 patent claims specific systems for certifying

[37] Mark A. Lemley, *Software Patents and the Return of Functional Claiming*, 2013 WISC. L. REV. 905 (2013).

authorization of a computer over a network. The patent teaches specific systems wherein the authorizing computer creates a public key pair comprising a new public key and a new private key, and creates an authorization certificate that certifies that a holder of the authorization certificate is authorized to perform an action referred to in the authorization certificate.

64. The '634 patent and its related domestic patent[38] have been cited by 254 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '634 patent as relevant prior art:

- NBC Universal, Inc.
- Adobe Systems, Inc.
- Nokia Corporation
- EMC Corporation
- Microsoft Corporation
- Fujitsu Limited
- International Business Machines Corporation
- Siemens AG
- Intel Corporation
- NCR Corporation
- Samsung Electronics Co., Ltd.
- France Telecom
- Oracle Corporation
- NEC Corporation
- Telefonaktiebolaget L.M. Ericsson
- Hewlett-Packard Company
- AT&T, Inc.
- Lucent Technologies, Inc.
- Intertrust Technologies Corporation
- General Electric Company
- Novell, Inc.
- General Electric Company
- Hitachi, Ltd.
- eBay, Inc.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,191,447

65. Soverain references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

[38] See U.S. Patent No. 6,490,358.

66. Apple designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for extracting data from sources of network-based information.

67. Apple designs, makes, sells, offers to sell, imports, and/or uses the Apple.com webstore (www.apple.com/shop/) (the "Apple '447 Product(s)").

68. On information and belief, one or more Apple subsidiaries and/or affiliates use the Apple '447 Products in regular business operations.

69. On information and belief, one or more of the Apple '447 Products include technology for extracting data from sources of network-based information in a communications network having a plurality of network servers programmed to transmit network-based information.

70. On information and belief, one or more of the Apple '447 Products enable an object embedding program implemented on a computer. The object embedding program contains functionality to locate a script program.

71. On information and belief, the Apple '447 Products execute an object embedding program implemented on a computer on a network (e.g., Apple Safari web browser). For example, web browsers such as Apple Safari (i.e., object embedding program) is executed on viewer computer that is connected to the internet.

72. On information and belief, the Apple '447 Products enable a web browser to locate a script program in the Apple website's HTML source files that are provided by Apple web servers. Apple Safari locates the embedded Javascript links. The script program URL is contained with the HTML source file of the webpage.

73. On information and belief, the Apple '447 Products enable script programs including external.js, familyselection-stack.js, mac-configurations-stack.js, step1modular.js, base-flex.js, productdetails-flex.js, etc.

74. On information and belief, the Apple '447 Products are available to businesses and individuals throughout the United States.

75. On information and belief, the Apple '447 Products are provided to businesses and individuals located in the Eastern District of Texas.

76. On information and belief, the Apple '447 Products comprise a system containing functionality for a script program that is implemented on a computer on a communication network.

77. On information and belief, the Apple '447 Products contain a script program wherein the script program is structured to extract data from network-based information provided by a networked server.

78. On information and belief, the Apple '447 Products contain an object embedding program, implemented on computers. The object embedding program implemented on the '447 Product comprises a link to said network-based information provided by a networked server.

```
! function t(e, n, i) {
    function r(a, s) {
        if (!n[a]) {
            if (!e[a]) {
                var c = "function" == typeof require && require;
                if (!s && c) return c(a, !0);
                if (o) return o(a, !0);
                var l = new Error("Cannot find module '" + a + "'");
                throw l.code = "MODULE_NOT_FOUND", l
            }
            var u = n[a] = {
                exports: {}
            };
            e[a][0].call(u.exports, function(t) {
                var n = e[a][1][t];
                return r(n ? n : t)
            }, u, u.exports, t, e, n, i)
        }
        return n[a].exports
    }
    for (var o = "function" == typeof require && require, a = 0; a <
        i.length; a++) r(i[a]);
    return r
}({
        1: [function(t, e, n) {
                var i = t("@aos/ac-store"),
                    r = t("./src/ApplePay.js"),
                    o = t("@aos/as-telemetry/src/telemetry.js");
                t("./src/security.js"), window.acStoreClearCache =
                    function() {
                        window.acStore && window.acStore.clearCache ?
                            window.acStore.clearCache(!0) : i.staticClearCache()
                    }, window.acStoreApplePay = r;
                var a = function() {
                    t("ac-globalnav/src/js/ac-globalnav"), t(
                        "@aos/ac-footer-dist"), r.init()
                };
                document.addEventListener ? document.addEventListener(
                        "DOMContentLoaded", a) : document.onreadystatechange =
                    function() {
```

Apple Store external.js Java Script Excerpt, APPLE.COM STORE WEBSITE VIEWED IN NETWORK INSPECTION VIEWER, available at: https://store.storeimages.cdn-apple.com/4974/store.apple.com/shop/rs-external/rel/external.js (last visited March 2017).

79. On information and belief, the Apple '447 Products enable an object embedding program to (via a link) locate a script program.

80. On information and belief, the Apple ‘447 Products enable an object embedding program that is structured to apply the script program to the network-based information. The application of the script program causes data to be extracted from a networked server. For example, the Apple website applies the script program to the network-based information which is provided by the Apple webservers linked by the link in the object embedding program. Browser such as Apple Safari execute a javascript program which in turn applies the RetailAvailability-SearchViewController function.

81. On information and belief, the Apple ‘447 Products enable the embedding of data in a compound document that is on the communications network.

82. On information and belief, the Apple ‘447 Products enable the object embedding program to locate the script program via a link. Further, the ‘447 Products enable the network-based information to be linked to the scripting program.

83. On information and belief, the Apple ‘447 Products comprise a system for executing an object embedding program to embed said data within a compound document implemented on a computer in said communications network.

84. On information and belief, Apple has directly infringed and continues to directly infringe the ‘447 patent by, among other things, making, using, offering for sale, and/or selling technology for extracting data from sources of network-based information, including but not limited to the Apple ‘447 Products, which include infringing technology for managing transfers of information in a communications network. Such products and/or services include, by way of example and without limitation, the Apple ‘447 Products.

85. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Apple ‘447 Products, Apple has injured Soverain and is liable to Soverain for directly infringing one or more claims of the ‘447 patent, including at least claim 5, pursuant to 35 U.S.C. § 271(a).

86. On information and belief, Apple also indirectly infringes the ‘447 patent by actively inducing infringement under 35 USC § 271(b).

87. On information and belief, Apple had knowledge of the ‘447 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the ‘447 patent and knew of its infringement, including by way of this lawsuit.

88. On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple ‘447 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘447 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘447 patent and with the knowledge that the induced acts would constitute infringement. For example, Apple provides the Apple ‘447 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘447 patent, including at least claim 5, and Apple further provides documentation and training materials that cause customers and end users of the Apple ‘447 Products to utilize the products in a manner that directly infringe one or more claims of the ‘447 patent. By providing instruction and training to customers and end-users on how to use the Apple ‘447 Products in a manner that directly infringes one or more claims of the ‘447 patent, including at least claim 5, Apple specifically intended to induce infringement of the ‘447 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple ‘447 Products, e.g., through Apple user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘447 patent. Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘447 patent, knowing that such use constitutes infringement of the ‘447 patent.

89. The ‘447 patent is well-known within the industry as demonstrated by the over 135 citations to the ‘447 patent in published patents and patent applications assigned to technology companies and academic institutions. Several of Apple’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘447 patent. To gain

advantage over Apple's competitors by utilizing the same licensed technology without paying reasonable royalties, Apple infringed the '447 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

90. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '447 patent.

91. As a result of Apple's infringement of the '447 patent, Soverain has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 8,935,706

92. Soverain references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

93. Apple designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing authentication credentials for access to data stored on servers.

94. Apple makes, sells, offers to sell, imports, and/or uses Apple iMessage ("iMessage").

95. Apple makes, sells, offers to sell, imports, and/or uses Apple FaceTime ("FaceTime").

96. Apple makes, sells, offers to sell, imports, and/or uses Apple Handoff ("Handoff").

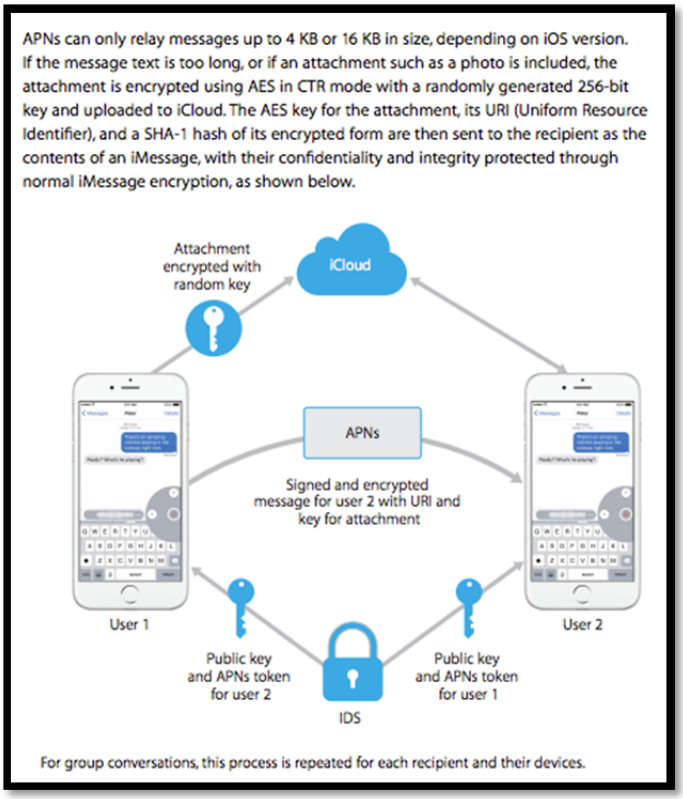
97. Apple makes, sells, offers to sell, imports, and/or uses Apple HomeKit ("HomeKit").

98. Apple makes, sells, offers to sell, imports, and/or uses Apple iOS mobile devices (e.g., iPhone, iPad, iPod Touch) ("iOS")

99. Apple designs, makes, sells, offers to sell, imports, and/or uses the applications, services, and devices: iMessage, FaceTime, Handoff, and iOS (collectively, the "Apple '706 Products").

100. On information and belief, one or more Apple subsidiaries and/or affiliates use the Apple '706 Products in regular business operations.

101. On information and belief, one or more of the Apple '706 Products include technology for managing authentication credentials for access to data stored on a network. Specifically, the Apple Products perform the managing of authentication credential to network based information by storing authentication data on Apple Servers. The below diagram shows how when User 1 is requesting information for User 2 (over a network) the authentication related credentials are stored on Apple Servers including the "iCloud."



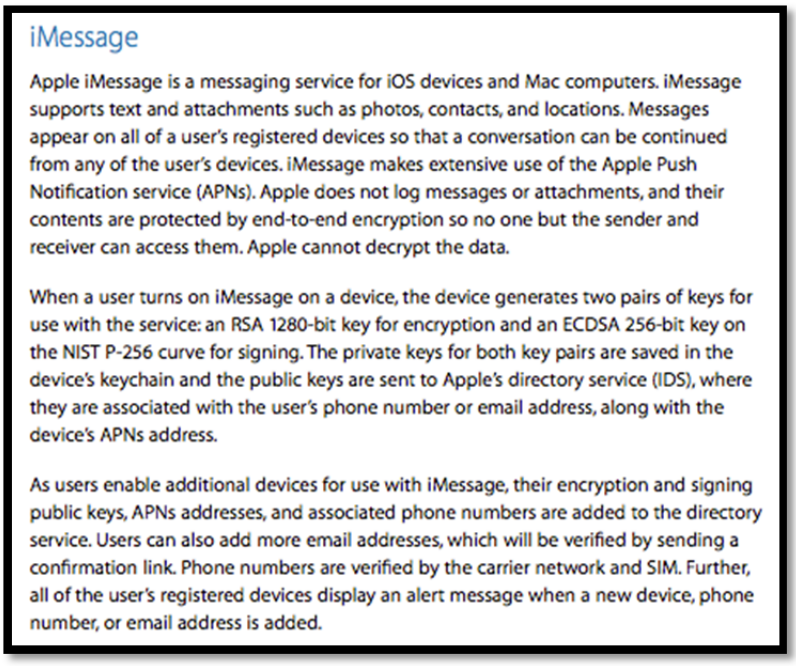
iOS Security Guide, APPLE WHITE PAPER at 62 (May 2016).

102. On information and belief, one or more of the Apple '706 Products include functionality for receiving and storing authentication credentials for each of the plurality of

sources of network based information. Specifically, the Apple '706 Products enable storing access credentials that relate to specific systems that are connected via a network.

103. On information and belief, one or more of the Apple '706 Products enable storing authentication credentials in a table of pairs. The table that is used by the '706 Products to store the credentials is organized so that each pair stored in the table represents a subscription service network server and corresponding credentials for the subscription service.

104. Specifically, Apple stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair, in a database. For example, an Apple iMessage server stores, in at least one database, a plurality of encrypted records (e.g., encrypted iMessage records), each encrypted record having an associated asymmetric encryption key pair (e.g., an associated RSA-1280 asymmetric key pair) and being encrypted with a first component (e.g., a private key component) of the associated asymmetric encryption key pair.



iMessage

Apple iMessage is a messaging service for iOS devices and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data.

When a user turns on iMessage on a device, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve for signing. The private keys for both key pairs are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which will be verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. Further, all of the user's registered devices display an alert message when a new device, phone number, or email address is added.

iOS Security Guide, APPLE WHITE PAPER at 41 (May 2016).

105. On information and belief, one or more of the Apple '706 Products enable forwarding access requests to a server where network based information is stored.

106. On information and belief, one or more of the Apple '706 Products enable receiving a request for authentication from a server where network based information is stored. The authentication request received by the Apple '706 Products related to the access request is forwarded to the server where the network based information is stored.

107. On information and belief, one or more of the Apple '706 Products, in response to an authentication request retrieve the stored authentication credentials that are specific to the server where the network based information is stored. For example, the Apple iMessage server receives asymmetric key information (e.g., device-specific RSA-1280 asymmetric key information), comprising at least asymmetric encryption key information and asymmetric decryption key information.

> The provisioning process begins with the user signing in to iCloud. Next, the iOS device asks the accessory to sign a challenge using the Apple Authentication Coprocessor that is built into all Built for HomeKit accessories. The accessory also generates prime256v1 elliptic curve keys, and ***the public key is sent to the iOS device along with the signed challenge and the X.509 certificate of the authentication coprocessor. These are used to request a certificate for the accessory from the iCloud provisioning server.*** The certificate is stored by the accessory, but it does not contain any identifying information about the accessory, other than it has been granted access to HomeKit iCloud remote access. The iOS device that is conducting the provisioning also sends a bag to the accessory, which contains the URLs and other information needed to connect to the iCloud remote access server. This information is not specific to any user or accessory.

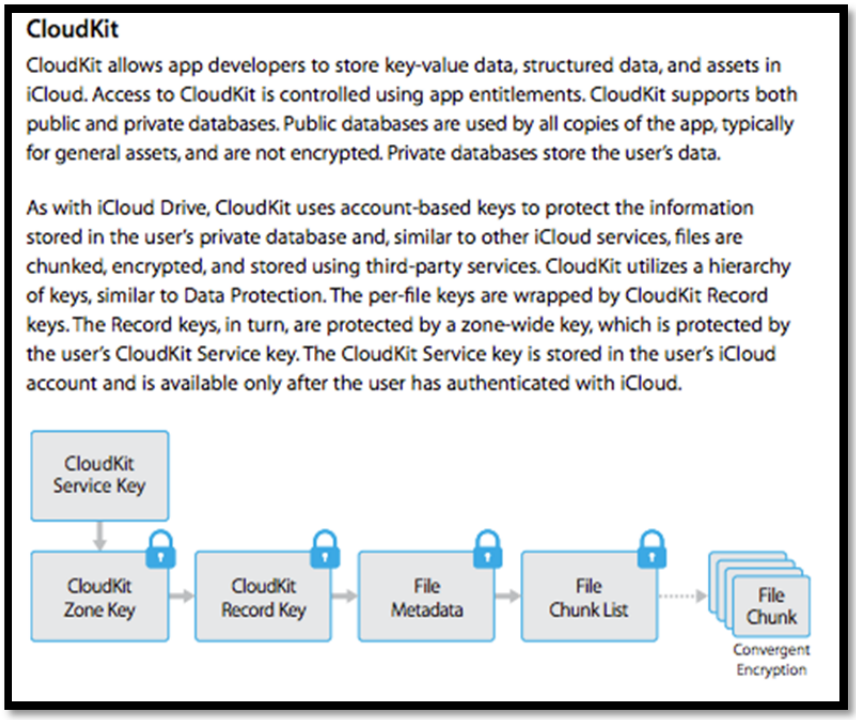
iOS Security Guide, APPLE WHITE PAPER at 23 (May 2016) (emphasis added).

108. On information and belief, one or more of the Apple '706 Products retrieve the authentication credentials that are assigned to a user upon registration with the subscription service.

109. On information and belief, one or more of the Apple '706 Products enable associating a password with stored authentication credentials.

110. On information and belief, one or more of the Apple ''706 Products enable receiving a password in response to a user initiating a network session with the network server. For example, HomeKit processes the information to invert the cryptographic function (e.g., the initial session-specific HomeKit cryptographic key, cipher suite, cryptographic mode of

operation, initial conditions, and/or other cryptographic comprehension information) and impose the new comprehension function (e.g., the new session-specific HomeKit cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information (e.g., the user and/or device-specific Ed25519 asymmetric key information), without providing the intermediary (e.g., the HomeKit framework intermediary) with sufficient asymmetric key information to decrypt the processed information. In addition, the Apple iCloud server outputs processed information (e.g., processed iCloud Drive, CloudKit, or iCloud Backup information) for receipt by a receiving third-party cloud storage server (e.g., Microsoft Azure) and/or one or more receiving iOS mobile devices (e.g., iPhone, iPad, and/or iPod Touch).



iOS Security Guide, APPLE WHITE PAPER at 43 (May 2016).

111. On information and belief, one or more of the Apple '706 Products enable transmitting authentication credentials to the server where network based information is stored.

The transmission of authentication credentials occurs in the Apple '706 Products following successful verification of the user's password.

112. On information and belief, the Apple '706 Products are provided to businesses and individuals located in the Eastern District of Texas.

113. On information and belief, one or more of the Apple '706 Products enable using a single password to authenticate a user for multiple sources of network based information (e.g., network based information stored on two different servers).

114. On information and belief, Apple has directly infringed and continues to directly infringe the '706 patent by, among other things, making, using, offering for sale, and/or selling technology for managing authentication credentials for access to a plurality of sources of network-based information, including but not limited to the Apple '706 Products, which include infringing authentication credential management technologies. Such products and/or services include, by way of example and without limitation, the Apple '706 Products.

115. By making, using, testing, offering for sale, and/or selling products and services for managing authentication credentials for access to a plurality of sources of network based information, including but not limited to the Apple '706 Products, Apple has injured Soverain and is liable to Soverain for directly infringing one or more claims of the '706 patent, including at least claims 1-5, pursuant to 35 U.S.C. § 271(a).

116. On information and belief, Apple also indirectly infringes the '706 patent by actively inducing infringement under 35 USC § 271(b).

117. On information and belief, Apple had knowledge of the '706 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Apple knew of the '706 patent and knew of its infringement, including by way of this lawsuit.

118. On information and belief, Apple intended to induce patent infringement by third-party customers and users of the Apple '706 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Apple specifically intended and was aware that the normal and customary

use of the accused products would infringe the ‘706 patent. Apple performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘706 patent and with the knowledge that the induced acts would constitute infringement. For example, Apple provides the Apple ‘706 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘706 patent, including at least claims 1-5, and Apple further provides documentation and training materials that cause customers and end users of the Apple ‘706 Products to utilize the products in a manner that directly infringe one or more claims of the ‘706 patent. By providing instruction and training to customers and end-users on how to use the Apple ‘706 Products in a manner that directly infringes one or more claims of the ‘706 patent, including at least claims 1-5, Apple specifically intended to induce infringement of the ‘706 patent. On information and belief, Apple engaged in such inducement to promote the sales of the Apple ‘706 Products, e.g., through Apple user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘706 patent. Accordingly, Apple has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘706 patent, knowing that such use constitutes infringement of the ‘706 patent.

119. The ‘706 patent is well-known within the industry as demonstrated by the over 135 citations to the ‘706 patent in published patents and patent applications assigned to technology companies and academic institutions. Several of Apple’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘706 patent. To gain an advantage over Apple’s competitors by utilizing the same licensed technology without paying reasonable royalties, Apple infringed the ‘706 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

120. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘706 patent.

121. As a result of Apple's infringement of the '706 patent, Soverain has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 5,708,780

122. Soverain references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

123. Apple designed, made, used, sold, and/or offered for sale in the United States products and/or services for processing service requests from a client to a server system through a network.

124. Apple designed, made, sold, offered to sell, imported, and/or used the infringing products that implement the NSURLSession Class and related classes which provide an API for downloading content including: iOS 7.0 and later, macOS 10.9 and later, tvOS 7.0 and later, and watchOS 2.0 and later (collectively, the "Apple '780 Products.").

125. On information and belief, one or more Apple subsidiaries and/or affiliates used the Apple '780 Products in regular business operations.

126. On information and belief, one or more of the Apple '780 Products include technology for processing service requests from a client to server system through a network. Specifically, the Apple Products perform the steps of requesting from a client to a server system by using the NSURLSession Class as described below.

> The NSURLSession class and related classes provide an API for downloading content via HTTP. This API provides a rich set of delegate methods for supporting authentication and gives your app the ability to perform background downloads when your app is not running or, in iOS, while your app is suspended. To use the NSURLSession API, your app creates a series of sessions, each of which coordinates a group of related data transfer tasks. For example, if you are writing a web browser, your app might create one session per tab or window. ***Within each session, your app adds a series of tasks, each of which represents a request for a specific URL (and for any follow-on URLs if the original URL returned an HTTP redirect).***

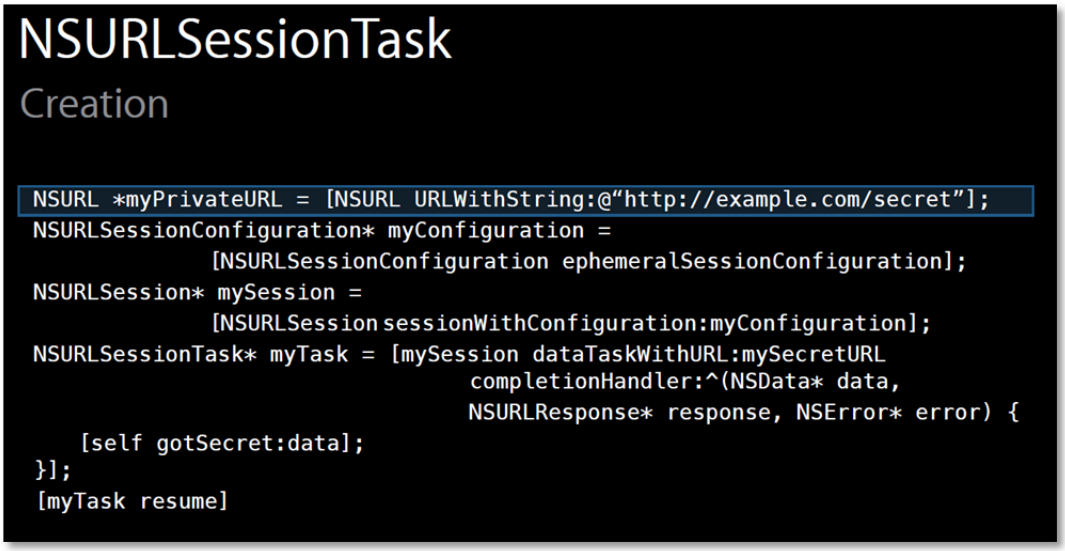
URL Session Programming Guide, APPLE GUIDES AND SAMPLE CODE, available at: https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/URLLoadingSystem/ (emphasis added).

127. On information and belief, one or more of the Apple '780 Products append to a path name in a uniform resource locator a session identifier. Specifically, the '780 Products tag, add, affix, or supplement to the sequence of zero or more elements that follows the host address in a URL a text string that identifies a session.

> To use the NSURLSession API, your app creates a series of sessions, each of which coordinates a group of related data transfer tasks. For example, if you are writing a web browser, your app might create one session per tab or window. Within each session, your app adds a series of tasks, each of which represents a request for a specific URL (and for any follow-on URLs if the original URL returned an HTTP redirect).

URL Session Programming Guide, APPLE GUIDES AND SAMPLE CODE, available at: https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/URLLoadingSystem/

128. On information and belief, one or more of the Apple '780 Products process service requests between a client and server using hypertext transfer protocol. Specifically, the '780 Products process service requests using a client/server protocol used to access information on the World Wide Web. As depicted in the below diagram from a presentation at the Apple World Wide Developers Conference described the process of a client retrieving data over a network by appending a unique SessionID to the URL path.



Steve Algernon, *What's New in Foundation Networking*, WWDC14 PRESENTATION at 60 (2014).

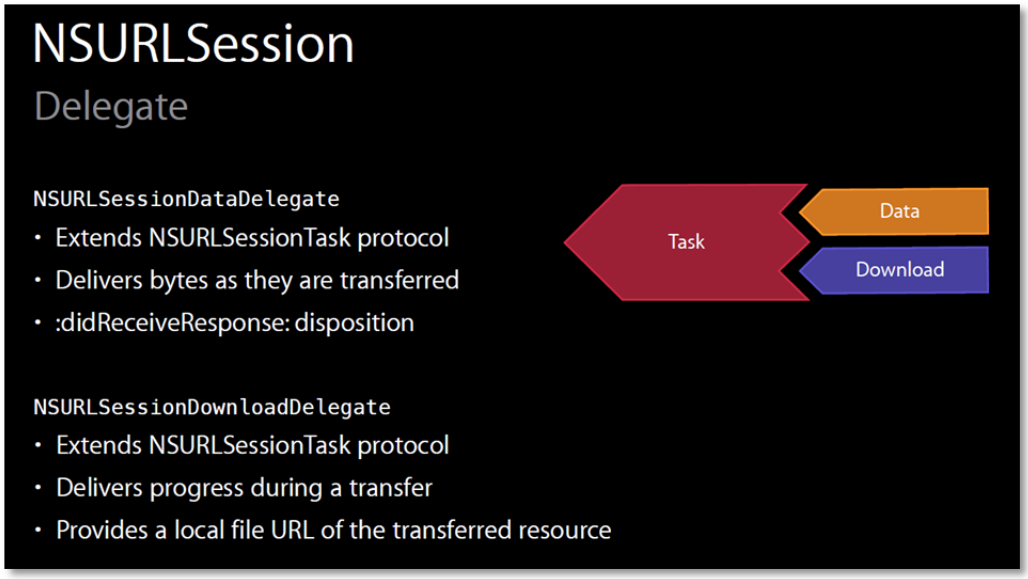
129. On information and belief, one or more of the Apple '780 Products return requests hypertext pages to a client in response to requests for hypertext pages received from the client through a network. Specifically, the '780 Products return requests for screen renderings referenced by (or including) hypertext links.

130. On information and belief, the Apple '780 Products then download from the server using an HTTP protocol. The response includes the data itself and metadata "describing the contents of the content data itself."

> The response from a server to a request can be viewed as two parts: metadata describing the contents and the content data itself. Metadata that is common to most protocols is encapsulated by the NSURLResponse class and consists of the MIME type, expected content length, text encoding (where applicable), and the URL that provided the response. Protocol-specific subclasses of NSURLResponse can provide additional metadata. For example, NSHTTPURLResponse stores the headers and the status code returned by the web server.

URL Session Programming Guide, APPLE GUIDES AND SAMPLE CODE, available at: https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/URLLoadingSystem/

131. On information and belief, the '780 Products respond to further client requests related to links in hypertext pages. Specifically, the '780 Products respond to requests from a client computer relating to a non-sequential web association which the user can use to navigate through related topics. For example, NSURLSession supports delegates which allow the transfer of hypertext pages related to a prior request. The below diagram shows this functionality.



Steve Algernon, *What's New in Foundation Networking*, WWDC14 PRESENTATION at 69 (2014).

132. On information and belief, the '780 Products track further requests from a client computer relating to a particular hypertext page. Specifically, the '780 Products track additional client computer requests for screen rendering referenced by (or including) hypertext links.

133. On information and belief, the '780 Products enable the use of a session identifier where the session identifier is a common session identifier and the server tracks client request within a session of requests.

134. On information and belief, the Apple '780 Products have been provided, sold, and/or offered for sale to businesses and individuals located in the Eastern District of Texas.

135. On information and belief, the '780 Products contain a means for receiving service requests from clients and for determining whether a service request includes a session identifier. Specifically, the '780 Products contain a content server as shown in the '780 patent specification at element 120 in Fig. 2A and element 52 in Fig. 3, executing a computer program implementing algorithm steps as shown in Fig. 2A, including block 104, and equivalent structures.

136. On information and belief, the '780 Products enable methods for controlling and monitoring access to network servers through the use of a session identifier. Further, the '780

Products utilize a session identifier that allows web servers to recognize and service multiple requests from the same client and control access to the server without repeated authentication.

137. On information and belief, the ‘780 Products contain a means for appending the session identifier as part of a path name in a uniform resource locator in response to an initial service request in a session of requests. Specifically, the ‘780 Products contain an authentication server as shown in the ‘780 Patent specification at element 200 in Figs. 2A and 2B, element 54 in Fig. 3, executing a computer program implementing algorithm steps as shown in Fig. 2B, including blocks 228, 230, and 232, and equivalent structures.

138. On information and belief, the ’780 Products comprise means for servicing service requests from a client which include a session identifier where subsequent service requests are processed in the session. Specifically, the ‘780 Products comprise a content server as shown in the ‘780 Patent specification at element 120 in Fig. 2A and element 52 in Fig. 3, executing a computer program implementing algorithm shown in Fig. 2A, including blocks 110, 112, and 116, or the client server exchange 9 and 10 in Fig. 3, and equivalent structures.

139. On information and belief, the ‘780 Products comprise a means for providing a session identifier. Specifically, the ‘780 Products comprise an authentication server as shown in the ’780 Patent specification at element 200 in Figs. 2A and 2B, and element 54 in Fig. 3, executing a computer program implementing algorithm steps as shown in Fig. 2B, including blocks 228, 230, and 232, and equivalent structures.

140. On information and belief, the ‘780 Products enable the use of a uniform resource locator that includes a transfer protocol identifier, a host name, one or more directory names, and a file name.

141. On information and belief, the ‘780 Products enable the use of session identifier where the session identifier is appended to the path name in the uniform resource locator between the transfer protocol identifier and the file name. Specifically, the ‘780 Products use a text string that identifies a series of requests and responses to perform a complete task or set of tasks between a client and a server system. The ‘780 Products tag, add, affix, or supplement the

text string that identifies a session to the sequence of zero or more elements that follows the host address in a URL between the transfer protocol identifier and file name.

142. On information and belief, the '780 Products comprise a server system that tracks access history information within a client-server session.

143. On information and belief, the '780 Products use a session identifier that enables the client to access files within a protected domain. Specifically, the '780 Products use a text string that identifies a session to enable a client computer to access files within a protected domain.

144. On information and belief, the '780 Products enable the use of a session identifier to access files with a plurality of servers.

145. On information and belief, the '780 Products enable the use of a client computer running a web browser (e.g., Safari) and a web server where the session of requests include hypertext transfer protocol GET requests transmitted from the web browser on the client computer to the web server. Further, the '780 Products use GET requests which include a uniform resource locator having the session identifier appended to it. Specifically, the GET requests include a text string that identifies a session where the text string is tagged, added, affixed, or supplemented to the URL as part of a path name.

146. On information and belief, Apple has directly infringed the '780 patent by, among other things, having made, used, offered for sale, and/or sold technology for processing service requests from a client to a server system over a computer network, including but not limited to the Apple '780 Products, which include infringing technologies for processing service requests from a client to a server system over a computer network. Such products and/or services include, by way of example and without limitation, the Apple '780 Products.

147. By having made, used, tested, offered for sale, and/or sold products and services for processing service requests from a client to a server system over a computer network, including but not limited to the Apple '780 Products, Apple has injured Soverain and is liable to

Soverain for directly infringing one or more claims of the ‘780 patent, including at least claims 22, 23, 32, 33, 112-114, 127, 128, and 129, pursuant to 35 U.S.C. § 271(a).

148. The ‘780 patent is well-known within the industry as demonstrated by the over 1,840 citations to the ‘780 patent in published patents and patent applications assigned to technology companies and academic institutions. Several of Apple’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘780 patent. To gain an advantage over Apple’s competitors by utilizing the same licensed technology without paying reasonable royalties, Apple infringed the ‘780 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

149. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘780 patent.

150. Because of Apple’s infringement of the '780 patent, Soverain has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 6,212,634

151. Soverain references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

152. Apple designed, made, used, sold, and/or offered for sale in the United States products and/or services for certifying authorizations between computers over a network.

153. Apple designed, made, sold, offered to sell, imported, and/or used the Apple iPad, iPhone, and iPod Touch devices running iOS Versions 9.0 and 10.0 (collectively, the Apple ‘634 Products).

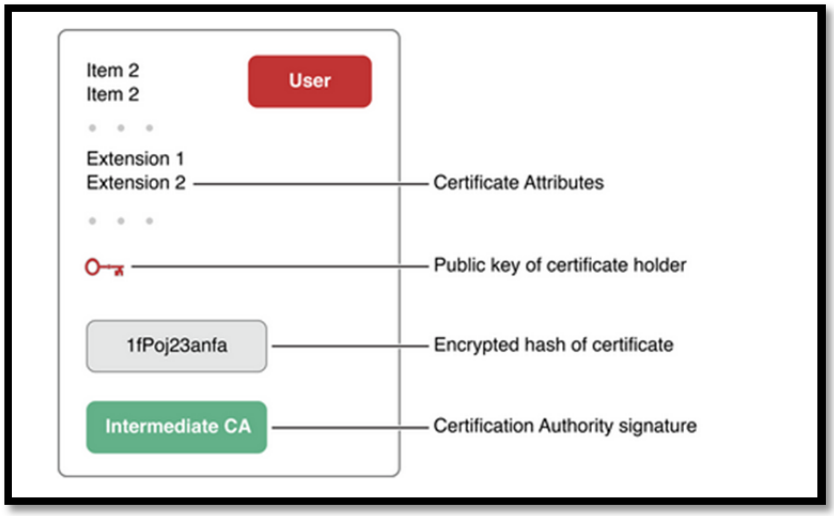
154. On information and belief, one or more Apple subsidiaries and/or affiliates used the Apple ‘634 Products in regular business operations.

155. On information and belief, one or more of the Apple '634 Products include technology for certifying authorizations between computers over a network. For example, the Apple Products enable intermediate certificates signed by a certificate authority that contain "Certificate Attributes" that identify:

> [A]ttributes of a digital certificate (known as *certificate extensions*) are said to establish a *level of trust* for a digital certificate. The level of trust for a certificate is used to answer the question 'Should I trust this certificate for this action?' A *trust policy* is a set of rules that specify how to evaluate a certificate to see if it is valid for a specific level of trust.

Certificate, Key, and Trust Services Programming Guide, APPLE DEVELOPER GUIDES AND SAMPLE CODE (January 28, 2013).

156. On information and belief, one or more of the Apple '634 Products create an authorization certificate that certifies that a holder of the authorization certificate is authorized to perform a particular action specified in the authorization certificate. The below diagram from Apple Product documentation shows for a certificate the use of "Extensions" or "Certificate Attributes" to identify what specific programs a user can access based on the values in the certificate.



Cryptographic Services Guide, APPLE DEVELOPER GUIDES AND SAMPLE CODE (July 7, 2015).

157. On information and belief, one or more of the Apple '634 Products create an authorization certificate that has a file structure that supports critical components and extension components.

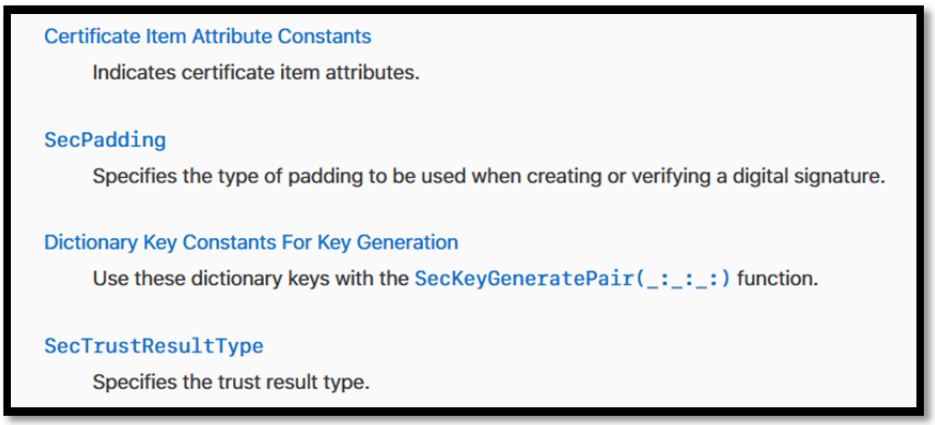
158. On information and belief, one or more of the Apple '634 Products cause the authorization certificate to be transmitted to the authorized computer. The authorized computer is programmed to accept certificates having file structures that support critical components and extension components. "The problem of ensuring that a public key actually belongs to the entity you want to authenticate can be addressed using digital certificates." *Authentication, Authorization, and Permissions Guide*, APPLE DEVELOPER GUIDES AND SAMPLE CODE (January 28, 2013).

159. Apple documentations describes that this occurs by sending the information to a server. "If you are using digital certificates for authentication—to authenticate a web server, for example—use the functions in Certificate, Key, and Trust Services." *Id.*

> A *digital certificate* is a collection of data used to verify the identity of the holder or sender of the certificate. For example, a certificate contains such information as:
>
> - Certificate issuer
> - Certificate holder
> - Validity period (the certificate is not valid before or after this period)
> - Public key of the owner of the certificate
> - *Certificate extensions*, which contain additional information such as allowable uses for the private key associated with the certificate
> - Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer

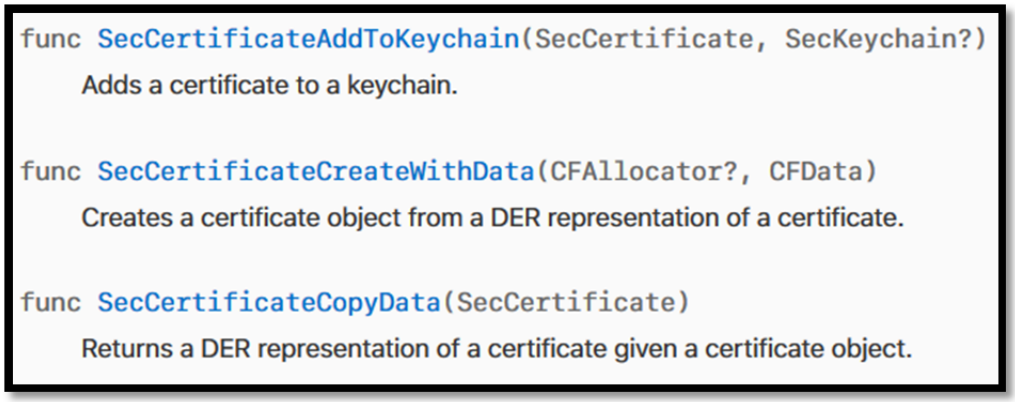
Certificate, Key, and Trust Services Programming Guide, APPLE DEVELOPER GUIDES AND SAMPLE CODE (January 28, 2013).

160. On information and belief, one or more of the Apple '634 Products cause the authorization certificate to be transmitted to an authorized computer that is programmed to accept the critical components but to reject certificates having file structures that support critical components and extension components when the authorized computer is not programmed to accept the critical components. For example, authorized computer is programmed to accept the critical components (identified above) but reject certificates that have a file structure that supports critical components and extension components. These can be performed by checking the Certificate item attribute constants.



Certificate, Key, and Trust Services, APPLE DEVELOPER API DOCUMENTATION (last visited January 2017) available at, https://developer.apple.com/reference/security/certificate_key_and_trust_services.

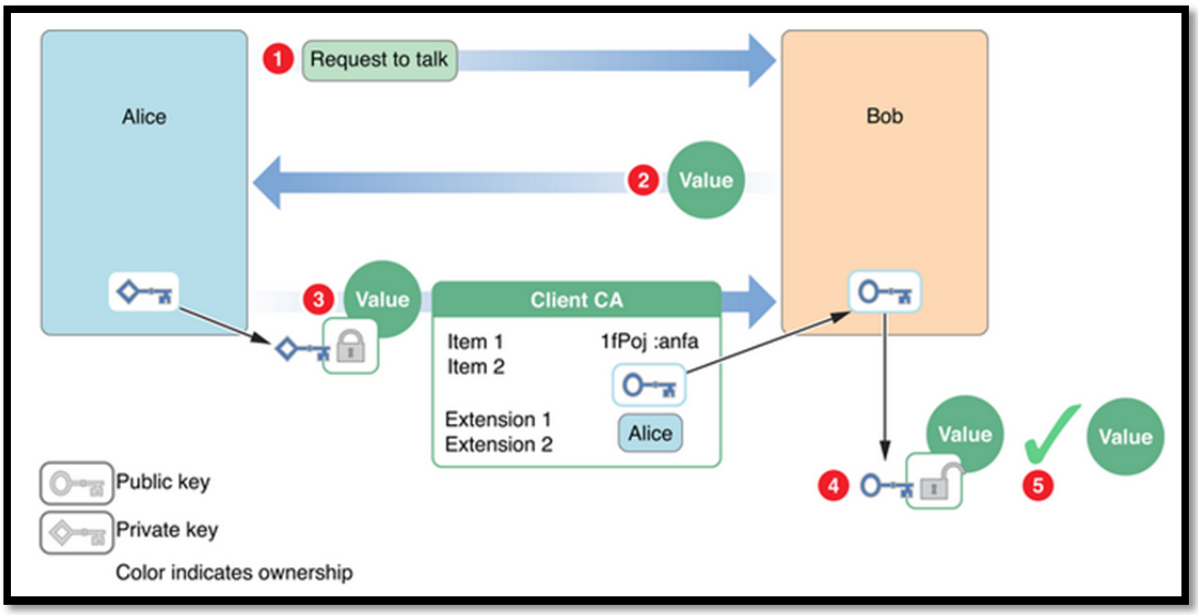
161. On information and belief, the Apple '634 Products enable creating an authorization certificate identifying what the client is authorized to perform relating to a specific action. These specific actions are contained in the "Certificate Extensions" of the certificate. Apple documentation describes functionality where the authorization certificate is created at the client computer.



Certificate, Key, and Trust Services, APPLE DEVELOPER API DOCUMENTATION (last visited January 2017) available at, https://developer.apple.com/reference/security/certificate_key_and_trust_services.

162. On information and belief, one or more of the Apple '634 Products include in the authorization certificate information that is unique to a particular action specified in the authorization certificate as at least one critical component of the authorization certificate. The

below diagram from Apple Product documentation shows the "Client CA" that is generated by the authorizing computer.



Authentication, Authorization, and Permissions Guide, APPLE DEVELOPER GUIDES AND SAMPLE CODE (January 28, 2013).

163. On information and belief, one or more of the Apple '634 Products include information unique to the particular action specified in the authorization certificate as at least one critical component of the authorization certificate in order to prevent the authorization certificate from being accepted by computers that are not programmed to accept the information unique to the action referred to in the authorization certificate.

164. On information and belief, the Apple '634 Products have been provided, sold, and/or offered for sale to businesses and individuals located in the Eastern District of Texas.

165. On information and belief, Apple has directly infringed the '634 patent by, among other things, having made, used, offered for sale, and/or sold technology for certifying authorizations between computers over a network, including but not limited to the Apple '634 Products, which include infringing technologies for certifying authorizations between computers over a network. Such products and/or services include, by way of example and without limitation, the Apple Products.

166. By having made, used, tested, offered for sale, and/or sold products and services for certifying authorizations between computers over a network, including but not limited to the Apple '634 Products, Apple has injured Soverain and is liable to Soverain for directly infringing one or more claims of the '634 patent, including at least claim 4, pursuant to 35 U.S.C. § 271(a).

167. The '634 patent is well-known within the industry as demonstrated by the over 196 citations to the '634 patent in published patents and patent applications assigned to technology companies and academic institutions. Several of Apple's competitors have paid considerable licensing fees for their use of the technology claimed by the '634 patent. To gain an advantage over Apple's competitors by utilizing the same licensed technology without paying reasonable royalties, Apple infringed the '634 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

168. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '634 patent.

169. Because of Apple's infringement of the '634 patent, Soverain has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Apple's infringement, but in no event less than a reasonable royalty for the use made of the invention by Apple together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Soverain respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff Soverain that Apple has infringed, either literally and/or under the doctrine of equivalents, the '447 patent, the '706 patent, the '780 patent, and the '634 patent;

B. An award of damages resulting from Apple's acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that Defendant's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant.

E. Any and all other relief to which Soverain may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Soverain IP, LLC requests a trial by jury of any issues so triable by right.

Dated: March 16, 2017

Respectfully submitted,

/s/ Dorian S. Berger

Elizabeth L. DeRieux
TX Bar No. 05770585
D. Jeffrey Rambin
TX Bar No. 00791478
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

OF COUNSEL:

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Attorneys for Soverain IP, LLC