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

DIGITALDOORS, INC.,

Plaintiff,

v.

INTERNATIONAL BUSINESS MACHINES CORPORATION,

Defendant.

Case No. 2:22-cv-457-JRG-RSP

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT AND JURY TRIAL DEMANDED

FIRST AMENDED COMPLAINT

This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code, against Defendant International Business Machines Corporation ("IBM" or "Defendant") that relates to seven U.S. patents owned by DigitalDoors, Inc. ("DigitalDoors" or "Plaintiff"): 7,313,825, 7,322,047, 7,349,987, 7,552,482, 7,721,344, 7,958,268, and 8,468,244 (collectively, the "Patents-in-Suit").

PARTIES

1. Plaintiff DigitalDoors is a Miami, Florida based company with a principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, Florida 33140.

2. IBM is a New York corporation with its principal place of business in Armonk, New York 10504. IBM's Registered Agent for service of process in Texas is CT Corp. System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

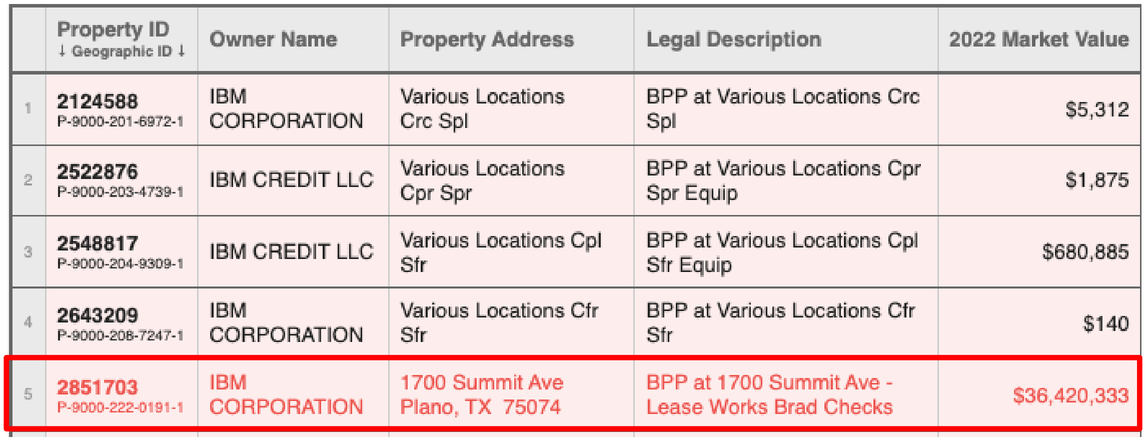
JURISDICTION AND VENUE

3. This is a civil action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*., and more particularly 35 U.S.C. § 271.

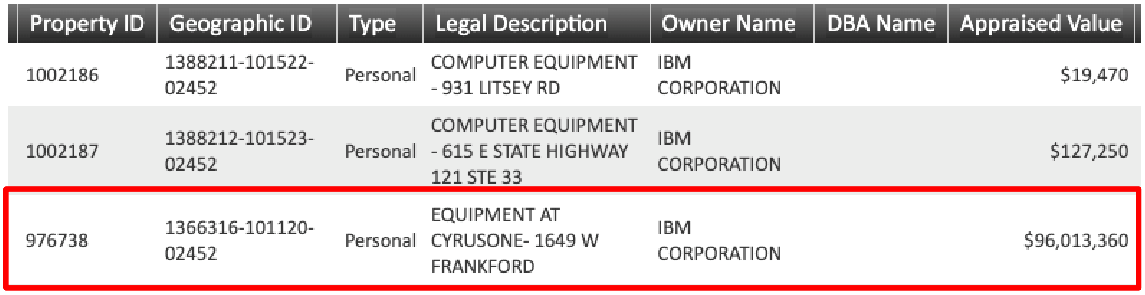
4. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a) in which the district courts have original and exclusive jurisdiction of any civil action for patent infringement.

5. IBM is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute because (i) IBM has done and continues to do business in Texas; (ii) IBM has committed and continues to commit acts of patent infringement in the State of Texas, including making, using, offering to sell, and/or selling accused products/services in Texas, and/or importing accused products/services into Texas, including via Internet sales, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein, and (iii) IBM is registered to do business in Texas.

6. Venue is proper in this district as to IBM pursuant to 28 U.S.C. § 1400(b). IBM has committed and continues to commit acts of patent infringement in this district, including making, using, offering to sell, and/or selling accused products/services in this district, and/or importing accused products/services into this district, including via Internet sales, inducing others to commit acts of patent infringement in this District, and/or committing at least a portion of any other infringements alleged herein in this District. IBM also has regular and established places of business in this District, including at 1700 Summit Ave, Plano, TX 75074 (as shown in the below screenshot from the Collin County Appraisal District site: https://www.collincad.org/propertysearch) and at 1649 W Frankford Rd, Carrollton, TX 75007 (as shown in the below screenshot from the Denton County Appraisal District site: https://www.dentoncad.com).



	Property ID ↓ Geographic ID ↓	Owner Name	Property Address	Legal Description	2022 Market Value
1	**2124588** P-9000-201-6972-1	IBM CORPORATION	Various Locations Crc Spl	BPP at Various Locations Crc Spl	$5,312
2	**2522876** P-9000-203-4739-1	IBM CREDIT LLC	Various Locations Cpr Spr	BPP at Various Locations Cpr Spr Equip	$1,875
3	**2548817** P-9000-204-9309-1	IBM CREDIT LLC	Various Locations Cpl Sfr	BPP at Various Locations Cpl Sfr Equip	$680,885
4	**2643209** P-9000-208-7247-1	IBM CORPORATION	Various Locations Cfr Sfr	BPP at Various Locations Cfr Sfr	$140
5	**2851703** P-9000-222-0191-1	IBM CORPORATION	1700 Summit Ave Plano, TX 75074	BPP at 1700 Summit Ave - Lease Works Brad Checks	$36,420,333



Property ID	Geographic ID	Type	Legal Description	Owner Name	DBA Name	Appraised Value
1002186	1388211-101522-02452	Personal	COMPUTER EQUIPMENT - 931 LITSEY RD	IBM CORPORATION		$19,470
1002187	1388212-101523-02452	Personal	COMPUTER EQUIPMENT - 615 E STATE HIGHWAY 121 STE 33	IBM CORPORATION		$127,250
976738	1366316-101120-02452	Personal	EQUIPMENT AT CYRUSONE- 1649 W FRANKFORD	IBM CORPORATION		$96,013,360

7. IBM has employees at 1700 Summit Ave, Plano, TX 75074, including at least a Data Center Technician. IBM is seeking employees at 1649 W Frankford Rd, Carrollton, TX 75007, including at least a Data Center Specialist.

BACKGROUND

8. DigitalDoors was established in 2001 to develop data security solutions for survivability and continuity of operations of the U.S. Government, including military and intelligence agencies. It evolved specifically towards the Pentagon's "Global Grid" communications infrastructure, and at the time, received enthusiastic reactions from leaders of the nation's national security apparatus.

9. The focus of DigitalDoors's technology is control of granular content in information flows. This control depends on the extraction of granular content elements from data streams and their dispersal into a distributed storage infrastructure. DigitalDoors then enables reconstruction of the granular content extracts back into the data stream based on the different

user identities, security clearance levels, and roles, subject to organizational policies. These technologies provide digital security, survivability, continuity, and secured sharing.

10. Over time, the private sector began to face the same sorts of issues as those that prompted DigitalDoors's innovations, securing large amounts of data from external and internal security threats.

11. Today, DigitalDoors's patented methodologies of data separation, dispersal, and reconstruction have become common practices for many companies. These companies use these methods to manage their cloud operations and private networks to provide defense for corporate and client data.

12. Other companies that cite to DigitalDoors patents in those companies' own patent applications indicate the degree to which the private sector has gravitated to the DigitalDoors patented solutions developed years earlier to protect national security. In 2019, for example, four DigitalDoors patents (all family members of the Patents-in-Suit) were among the 100 most-cited U.S. Patents.

13. IBM is one such company that has adopted the DigitalDoors technology.

14. In November 2015, IBM acquired Cleversafe, Inc. for $1.3 billion. Cleversafe was an object-storage solution provider that launched in 2004, years after DigitalDoors and its innovations. On information and belief, the Cleversafe solutions form the foundation for IBM's Cloud Object Storage technology today.

15. Together, DigitalDoors patents have been cited in IBM's and Cleversafe's own patents over 4,800 times.

THE PATENTS-IN-SUIT AND CLAIMS-IN-SUIT

16. DigitalDoors is the owner of record and assignee of each of U.S. Patent Nos. 7,313,825, ("the '825 Patent," attached as Exhibit A), 7,322,047 ("the '047 Patent," attached as Exhibit B), 7,349,987 ("the '987 Patent," attached as Exhibit C), 7,552,482 ("the '482 Patent," attached as Exhibit D), 7,721,344 ("the '344 Patent," attached as Exhibit E), 7,958,268 ("the '268 Patent," attached as Exhibit F), and 8,468,244 ("the '244 Patent," attached as Exhibit G) (collectively, the "Patents-in-Suit"). The claims in the Counts in this complaint are example claims; at least these patent claims are infringed by IBM.

17. DigitalDoors has the exclusive right to sue and the exclusive right to recover damages for infringement of the Patents-in-Suit during all relevant time periods.

18. On December 25, 2007, the '825 Patent, entitled "Data security system and method for portable device" was duly and legally issued by the USPTO.

19. On January 22, 2008, the '047 Patent, entitled "Data security system and method associated with data mining," was duly and legally issued by the USPTO.

20. On March 25, 2008, the '987 Patent, entitled "Data security system and method with parsing and dispersion techniques," was duly and legally issued by the USPTO.

21. On June 23, 2009, the '482 Patent, entitled "Data security system and method," was duly and legally issued by the USPTO.

22. On May 18, 2010, the '344 Patent, entitled "Data security system and method," was duly and legally issued by the USPTO.

23. On June 7, 2011, the '268 Patent, entitled "Data security system and method adjunct to a browser, telecom or encryption program," was duly and legally issued by the USPTO.

24. On June 18, 2013, the ’244 Patent, entitled “Digital information infrastructure and method for security designated data and with granular data stores,” was duly and legally issued by the USPTO.

25. The claims of the DigitalDoors patents improve computer functionality by resolving technological limitations with other data-security methods. One limitation is that traditional methods of restricting data access followed a binary “all-or-nothing” approach: one could either access the entire document, or none of it, curtailing the utility of the data and preventing multiple users from accessing different parts of data. Relatedly, those data-control mechanisms did not stop the user from distributing the data to other parties. Encryption burdens computer systems with high performance overhead (e.g., processing power and speed), and its use is limited to computers on both the storage/sender and viewing/receiver end with the requisite performance and resultant decryption capabilities. In addition, storing data files in their entirety in single locations makes them vulnerable to hacking, as one need only breach security measures for that location to access the files. Finally, these security measures do nothing to enhance the survivability of the networks’ data. The inventions in DigitalDoors’s asserted claims provide data security in a different fashion, avoiding these technological limitations.

26. The claims of the DigitalDoors patents solve these problems and address these vulnerabilities with pre-existing data storage and data-security technologies in unconventional ways. DigitalDoors provides data security by parsing data granularly, storing different pieces of data in separate stores, assigning different security clearance levels to users, and then permitting either partial or full reconstruction of the parsed data only in the presence of corresponding security clearances. The ordered combination of these different steps provides the claims with the necessary inventive concept. Features of DigitalDoors’s patented inventions include

distributed stored of data slices and multiple security levels. The combined elements of the DigitalDoors claims concern specific, discrete implementations that carry no risk of monopolizing data security, or even distributed storage for security. These elements require unconventional elements such as a plurality of physically distinguishable memories for storage of different document slices, a plurality of security levels for subsets of security sensitive words, characters, or icons, and/or permitting full or partial reconstruction only in the presence of predetermined security clearance. The particular arrangement of claim elements are technical improvements over prior art and were not routine, well-understood, or conventional.

IBM'S INFRINGING PRODUCTS AND SERVICES

27. IBM has been, and now is, directly infringing claims of the Patents-in-Suit under 35 U.S.C. § 271(a) by making, using, offering for sale, selling, and/or importing the below accused IBM Cloud Object Storage products/services in this District and elsewhere in the United States that include the software claimed in the Patents-in-Suit and/or by using the methods claimed in the Patents-in-Suit, including, for example, IBM's set-up, testing, demonstration, and operation of its IBM Cloud Object Storage products/services.

28. IBM Cloud Object Storage is a storage product/service used to store unstructured data and designed for high durability, resiliency, and security. IBM Cloud Object Storage uses object storage databases that contain two tables. The first table is an object directory table that contains the metadata about each stored object. The second table is the object storage table that contains the object data. The data (fixed digital content such as video and image files or large libraries of documents) is stored in the object store, while the metadata (contextual information about the data) is stored in a database/object directory table.

29. IBM has been and now is infringing, directly and by inducement, at least the following fifty four (54) claims of the Patents-in-Suit in this District and elsewhere in the United States:

- Claim 81 of the ’825 Patent
- Claims 1, 2, 10, 15, 16, 19, 33, 34, 42, 47, 48, and 51 of the ’047 Patent
- Claims 1, 6, 9, 10, 11, 15, 16, 21, 22, 23, and 27 of the ’987 Patent
- Claims 1, 5, 25, 26, 30, and 50 of the ’482 Patent
- Claims 1, 2, 3, 4, 5, 8, 16, 39, 40, 41, 43, 52, 53, 55, 79, 80, 82, 106, 107, and 113 of the ’344 Patent
- Claims 31, 36, and 41 of the ’268 Patent
- Claim 1 of the ’244 Patent

30. To the extent that IBM continues to provide these products and services and guidance to users, IBM has been and will be inducing the direct infringement of claims of the Patents-in-Suit pursuant to U.S.C. § 271(b) at least by one or more of making, using, offering for sale, selling and/or importing the below accused IBM Cloud Object Storage products/services in this District and elsewhere in the United States that were designed and intended to use and/or practice the methods and processes covered by the claims of the Patents-in-Suit. Further, various IBM user guides and product documentation, such as https://www.redbooks.ibm.com/redbooks/pdfs/sg248439.pdf and https://www.redbooks.ibm.com/redbooks/pdfs/sg248385.pdf, other support materials, and services and advertisement of features that are used and benefits that are achieved through use of the Patents-in-Suit have and will continue to induce infringement. IBM directs its customers to use IBM Cloud Object Storage products/services in an infringing manner by encouraging users

to "securely store large volumes of unstructured data" (https://www.ibm.com/cloud/blog/keeping-your-data-secure-with-ibm-cloud-object-storage) in a variety of manners that fall within the scope of the asserted claims.

31. IBM's continued provision of these products, services, and materials/guidance will demonstrate IBM's specific intent to cause and encourage direct infringement of the Patents-in-Suit with affirmative intent or willful blindness that such activities occur and knowledge that they constitute direct infringement of claims of the Patents-in-Suit.

32. IBM's infringement of claims of the Patents-in-Suit has been and continues to be willful. IBM has had actual knowledge of the Patents-in-Suit and DigitalDoors's claimed technology based in part on its interactions with DigitalDoors in 2010.

33. In 2010, Ron Redlich, an inventor of the DigitalDoors technology and President of DigitalDoors, Inc., met with several IBM representatives, and in the course of the ensuing communications, Mr. Redlich notified IBM of DigitalDoors's "large portfolio of patents." IBM subsequently asked Mr. Redlich detailed questions about patents in his portfolio but was unwilling to sign a nondisclosure agreement with DigitalDoors.

34. Additionally, IBM and its 2015 acquisition, Cleversafe, knew about DigitalDoors's patents from their being cited during prosecution of IBM's and Cleversafe's own patents. As noted previously, they cited DigitalDoors patents over 4,800 times. Of those over 4,800 instances, over 4,300 were citations to family members of the Patents-in-Suit. And the specific Patents-in-Suit also are repeatedly cited in IBM and Cleversafe patents:

DigitalDoors Patent No.	Cleversafe Citations	IBM Citations	Total
7,313,825	1	22	23
7,322,047	2	20	22
7,349,987	0	18	18
7,552,482	0	1	1
7,721,344	0	7	7
7,958,268	3	14	17
8,468,244	10	223	233

COUNT 1: INFRINGEMENT OF PAT. 7,313,825 CLAIM 81

35. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

36. Claim 81 of the ’825 Patent provides:

Preamble	A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores, said computer system having at least one portable computing device locatable with current location data, comprising:
Element A	determining when said portable computing device is within a predetermined region based upon said current location data;
Element B	permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

37. IBM directly infringes claim 81 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

38. IBM COS as a Service stores data that comprises words, characters, data objects or icons. Some of that data is security sensitive.

39. IBM COS as a Service provides a computer system that includes a plurality of memories. These memories comprise the various nodes that store slices of customer data. Nodes can serve as extract stores.

40. On Information and belief, there are pluralities of these extract stores with the multiple types of security access controls, implemented as discussed herein.

41. IBM COS as a Service stores user data as objects in buckets.

42. IBM COS as a Service implements security levels for data in multiple ways.

43. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Access for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

44. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

45. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

46. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

47. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

48. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

49. On information and belief, the IBM COS as a Service computer system is sometimes networked with portable computing devices, including mobile phones/tablets and/or laptops. These devices must provide their current location for IBM to implement context-based access restrictions.

50. IBM COS as a Service can use context-based restrictions to secure resources based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context. The context includes the network location of access requests.

51. IBM COS as a Service uses a portable device's current location to determine if the device is within a predetermined region and therefore able to access the data.

52. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data and the current location of the portable device allows retrieval of data from the nodes containing the security sensitive content.

53. That security clearance may be via ACLs, IAM, and/or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

54. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

55. The technology claimed in claim 81 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

56. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 2: INFRINGEMENT OF PAT. 7,322,047 CLAIM 1

57. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

58. Claim 1 of the '047 Patent provides:

Preamble	A method of securing data based upon a plurality of security levels, each with a predetermined security clearance, in a computer system having a

	plurality of computers therein and a plurality of memories designated as a remainder store and a plurality of extract stores for respective ones of said plurality of security levels operatively coupled over a communications network, said data having security sensitive content represented by one or more security sensitive words, data objects, characters, images, data elements or icons, comprising:
Element A	extracting said security sensitive content from said data to obtain (a) subsets of extracted data and (b) remainder data;
Element B	storing said extracted data and said remainder data in respective extract stores, corresponding to the respective security level of the extracted data, and said remainder store, respectively; and,
Element C	permitting reconstruction of some or all of said data via one or more of said subsets of extracted data from respective extract stores and remainder data only in the presence of predetermined security clearance for said respective security level corresponding to said respective extract stores.

59. IBM directly infringes claim 1 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

60. IBM COS as a Service stores user data as objects in buckets.

61. IBM COS as a Service implements security levels with predetermined security clearances for data in multiple ways.

62. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

63. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security

levels ("roles") of the data (objects and/or buckets).

64. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

65. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

66. IBM COS as a Service provides a network of computers that includes a plurality of memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

67. IBM COS as a Service stores data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

68. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

69. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding

security clearance as discussed previously.

70. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

71. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

72. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

73. The technology claimed in claim 1 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

74. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 3: INFRINGEMENT OF PAT. 7,322,047 CLAIM 2

75. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

76. Claim 2 of the '047 Patent provides:

Element A	A method of securing data as claimed in claim 1 operating over a plurality of computers interconnected together.

77. IBM directly infringes claim 2 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

78. IBM COS as a Service operates over a plurality of servers that are interconnected together. These servers are also connected to user device computers that access IBM COS as a Service.

79. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

80. The technology claimed in claim 2 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities,

provided a technological solution to a technological problem rooted in computer technology.

81. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 4: INFRINGEMENT OF PAT. 7,322,047 CLAIM 10

82. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

83. Claim 10 of the '047 Patent provides:

Element A	A method of securing data as claimed in claim 1 wherein said reconstruction partially reconstructs said data in response to a query and represents data mining of said data.

84. IBM directly infringes claim 10 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

85. IBM COS as a Service divides data into slices. These slices can be retrieved to partially reconstruct the data.

86. IBM COS supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

87. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to mine the required data slices for at least part of an object.

88. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object

Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

89. The technology claimed in claim 10 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

90. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 5: INFRINGEMENT OF PAT. 7,322,047 CLAIM 15

91. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

92. Claim 15 of the '047 Patent provides:

Preamble	A computerized method of securing data based upon a plurality of security levels, each with a predetermined security clearance, in memories designated as a remainder store and a plurality of extract stores for respective ones of said plurality of security levels, said data having security sensitive content represented by one or more security sensitive words, data objects, characters, images, data elements or icons, comprising:
Element A	extracting said security sensitive content from said data to obtain subsets of extracted data and remainder data;
Element B	storing said extracted data and said remainder data in respective extract stores, corresponding to the respective security level of the extracted data, and said remainder store, respectively; and,

Element C	permitting reconstruction of some or all of said data via one or more of said subsets of extracted data from respective extract stores and remainder data only in the presence of predetermined security clearance for said respective security level corresponding to said respective extract stores.

93. IBM directly infringes claim 15 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

94. IBM COS as a Service stores user data as objects in buckets.

95. IBM COS as a Service implements security levels with predetermined security clearances for data in multiple ways.

96. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

97. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets.

98. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

99. On information and belief, these various technologies often operate in conjunction

with each other, adding security levels and clearances.

100. IBM COS as a Service includes a plurality of memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores.

101. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

102. IBM COS as a Service stores data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

103. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

104. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

105. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

106. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

107. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

108. The technology claimed in claim 15 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

109. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 6: INFRINGEMENT OF PAT. 7,322,047 CLAIM 16

110. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

111. Claim 16 of the '047 Patent provides:

Element A	A method of securing data as claimed in claim 15 operating over a plurality of computers interconnected together.

112. IBM directly infringes claim 16 by practicing every step of the claimed method

when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

113. IBM COS as a Service operates over a plurality of servers that are interconnected together. These servers are also connected to user device computers that access IBM COS as a Service.

114. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

115. The technology claimed in claim 16 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

116. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 7: INFRINGEMENT OF PAT. 7,322,047 CLAIM 19

117. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

118. Claim 19 of the ’047 Patent provides:

Element A	A method of securing data as claimed in claim 15 wherein said reconstruction partially reconstructs said data in response to a query and represents data mining of said data.

119. IBM directly infringes claim 19 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

120. IBM COS as a Service divides data into slices. These slices can be retrieved to partially reconstruct the data.

121. IBM COS supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

122. When the client application issues a “read request,” the Accesser node instructs the Slicestor nodes to mine the required data slices for at least part of an object.

123. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

124. The technology claimed in claim 19 was not well understood, routine, or

conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

125. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 8: INFRINGEMENT OF PAT. 7,322,047 CLAIM 33

126. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

127. Claim 33 of the '047 Patent provides:

Preamble	A computer readable storage medium containing programming instructions for securing data based upon a plurality of security levels, each with a predetermined security clearance, in a computer system having a plurality of computers therein and a plurality of memories designated as a remainder store and a plurality of extract stores for respective ones of said plurality of security levels operatively coupled over a communications network, said data having security sensitive content represented by one or more security sensitive words, data objects, characters, images, data elements, or icons, the programming instructions comprising:
Element A	extracting said security sensitive content from said data to obtain (a) subsets of extracted data and (b) remainder data;
Element B	storing said extracted data and said remainder data in respective extract stores, corresponding to the respective security level of the extracted data, and said remainder store, respectively; and,
Element C	permitting reconstruction of some or all of said data via one or more of said subsets of extracted data from respective extract stores and remainder data only in the presence of predetermined security clearance for said respective security level corresponding to said respective extract stores.

128. IBM directly infringes claim 33 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also

by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

129. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

130. IBM COS as a Service and IBM COS on premises implement security levels with predetermined security clearances for data in multiple ways.

131. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

132. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

133. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

134. IBM COS as a Service and IBM COS on premises provide a network of computers that includes a plurality of memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores. These instructions provide for pluralities of these extract stores in IBM COS as a Service and in IBM COS on premises for the security levels associated with the multiple types of security clearances above.

135. IBM COS as a Service and IBM COS on premises store data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

136. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

137. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. These instructions also enable access to the stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

138. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They enable reconstruction of a full object or a part of an object while providing the appropriate

security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

139. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combine the slices including slices with security sensitive content and slices without security sensitive content.

140. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

141. The technology claimed in claim 33 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

142. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 9: INFRINGEMENT OF PAT. 7,322,047 CLAIM 34

143. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

144. Claim 34 of the '047 Patent provides:

Element A	A medium with programming instructions as claimed in claim 33 including programming instructions to store said extracted data and said remainder data over a plurality of computers interconnected together.

145. IBM directly infringes claim 34 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

146. IBM COS as a Service and IBM COS on premises divide data into slices, which are stored over a plurality of nodes.

147. IBM COS as a Service and IBM COS on premises store extracted and remainder data over a plurality of servers that are interconnected together. These servers are also connected to user device computers that access IBM COS as a Service and IBM COS on premises.

148. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

149. The technology claimed in claim 34 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

150. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 10: INFRINGEMENT OF PAT. 7,322,047 CLAIM 42

151. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

152. Claim 42 of the ’047 Patent provides:

Element A	A medium with programming instructions as claimed in claim 33 wherein said reconstruction partially reconstructs said data in response to a query and represents data mining of said data.

153. IBM directly infringes claim 42 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

154. IBM COS as a Service and IBM COS on premises divide data into slices. These slices can be retrieved to partially reconstruct the data.

155. IBM COS supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

156. When the client application issues a “read request,” the Accesser node instructs the Slicestor nodes to mine the required data slices for at least part of an object.

157. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its

customers to set up and use its systems to operate in an infringing manner.

158. The technology claimed in claim 42 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

159. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 11: INFRINGEMENT OF PAT. 7,322,047 CLAIM 47

160. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

161. Claim 47 of the '047 Patent provides:

Preamble	A computer readable storage medium containing programming instructions for securing data based upon a plurality of security levels, each with a predetermined security clearance, in a plurality of memories designated as a remainder store and a plurality of extract stores for respective ones of said plurality of security levels, said data having security sensitive content represented by one or more security sensitive words, data objects, characters, images, data elements or icons, comprising:
Element A	extracting said security sensitive content from said data to obtain (a) subsets of extracted data and (b) remainder data;
Element B	storing said extracted data and said remainder data in respective extract stores, corresponding to the respective security level of the extracted data, and said remainder store, respectively; and,
Element C	permitting reconstruction of some or all of said data via one or more of said subsets of extracted data from respective extract stores and remainder data only in the presence of predetermined security clearance for said respective security level corresponding to said respective extract stores.

162. IBM directly infringes claim 47 by setting up and operating IBM Cloud Object

Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

163. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

164. IBM COS as a Service and IBM COS on premises implement security levels with predetermined security clearances for data in multiple ways.

165. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

166. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

167. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or

service references.

168. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

169. IBM COS as a Service and IBM COS on premises include a plurality of memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores. These instructions provide for pluralities of these extract stores in IBM COS as a Service and in IBM COS on premises for the security levels associated with the multiple types of security clearances discussed above.

170. IBM COS as a Service and IBM COS on premises store data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

171. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

172. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

173. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They

enable reconstruction of a full object or a part of an object while providing the appropriate security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

174. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combines the slices including slices with security sensitive content and slices without security sensitive content.

175. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

176. The technology claimed in claim 47 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

177. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 12: INFRINGEMENT OF PAT. 7,322,047 CLAIM 48

178. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

179. Claim 48 of the '047 Patent provides:

Element A	A medium with programming instructions as claimed in claim 47 operating over a plurality of computers interconnected together.

180. IBM directly infringes claim 48 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

181. IBM COS as a Service and IBM COS on premises operate over a plurality of servers that are interconnected together. These servers are also connected to user device computers that access IBM COS as a Service and IBM COS on Premises.

182. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

183. The technology claimed in claim 48 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

184. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 13: INFRINGEMENT OF PAT. 7,322,047 CLAIM 51

185. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as

though set forth fully here.

186. Claim 51 of the ’047 Patent provides:

Element A	A medium with programming instructions as claimed in claim 47 wherein said reconstruction partially reconstructs said data in response to a query and represents data mining of said data.

187. IBM directly infringes claim 51 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

188. IBM COS as a Service and IBM COS on premises divide data into slices. These slices can be retrieved to partially reconstruct the data.

189. IBM COS supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

190. When the client application issues a “read request,” the Accesser node instructs the Slicestor nodes to mine the required data slices for at least part of an object.

191. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

192. The technology claimed in claim 51 was not well understood, routine, or

conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

193. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 14: INFRINGEMENT OF PAT. 7,349,987 CLAIM 1

194. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

195. Claim 1 of the '987 Patent provides:

Preamble	A method of securing data having one or more security sensitive words, characters or icons in a computer system with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:
Element A	extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;
Element B	storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and,
Element C	permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

196. IBM directly infringes claim 1 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

197. IBM COS as a Service stores data that comprises words, characters, or icons. Some of that data is security sensitive.

198. IBM COS as a Service provides a computer system with a plurality of physically distinguishable memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores.

199. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed herein.

200. IBM COS as a Service stores user data as objects in buckets.

201. IBM COS as a Service implements security levels for data in multiple ways.

202. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

203. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

204. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

205. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

206. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

207. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

208. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

209. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

210. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement

and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

211. The technology claimed in claim 1 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

212. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 15: INFRINGEMENT OF PAT. 7,349,987 CLAIM 6

213. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

214. Claim 6 of the '987 Patent provides:

Element A	A method as claimed in claim 1 including establishing a plurality of security levels each with a respective security clearance, each said subset of said security sensitive words, characters or icons being correlated with said plurality of security levels and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

215. IBM directly infringes claim 6 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

216. IBM COS as a Service establishes a plurality of security levels. On Information and belief, there are pluralities of these security levels associated with the multiple types of security clearances discussed herein.

217. IBM COS as a Service uses access control lists (ACLs) to correlate security clearances to the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

218. IBM COS as a Service divides data into slices. These slices can be retrieved to partially reconstruct the data.

219. IBM COS as a Service supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances to permit for a plurality of partial reconstructions.

220. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

221. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

222. The technology claimed in claim 6 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

223. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 16: INFRINGEMENT OF PAT. 7,349,987 CLAIM 9

224. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

225. Claim 9 of the '987 Patent provides:

Element A	A method as claimed in claim 1 including assessing a charge for extracting, storing or permitting reconstruction.

226. IBM directly infringes claim 9 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

227. IBM COS as a Service assesses a charge for use of the service (e.g., extracting, storing or permitting reconstruction) in at least some instances. By enabling "container mode" the system then supports tracking usage across users and assessing charges for services.

228. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to

operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

229. The technology claimed in claim 9 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

230. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 17: INFRINGEMENT OF PAT. 7,349,987 CLAIM 10

231. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

232. Claim 10 of the '987 Patent provides:

Preamble	A method of securing data with a parsing algorithm via a computer system having physically distinguishable memories designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:
Element A	parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;
Element B	storing said extracted data and said remainder data in said extract stores and said remainder store, respectively; and,
Element C	permitting full or partial reconstruction of said data via said extracted data from said respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

233. IBM directly infringes claim 10 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

234. IBM COS as a Service secures data with a parsing algorithm by splitting the data. IBM COS as a Service Accesser nodes split the data using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices."

235. IBM COS as a Service includes a plurality of physically distinguishable memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores.

236. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed herein.

237. IBM COS as a Service stores data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

238. IBM COS as a Service stores user data as objects in buckets.

239. IBM COS as a Service implements security levels for data in multiple ways.

240. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

241. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

242. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

243. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

244. IBM COS as a Service Accesser nodes parses the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices with associated security levels but not others.

245. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance associated with the security level.

246. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

247. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

248. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

249. The technology claimed in claim 10 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

250. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 18: INFRINGEMENT OF PAT. 7,349,987 CLAIM 11

251. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

252. Claim 11 of the '987 Patent provides:

Element A	A method as claimed in claim 10 wherein the step of parsing parses the data granularly.

253. IBM directly infringes claim 11 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

254. IBM COS as a Service Accesser nodes parses the data using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." The original data is divided on a granular level, sending small subsets of data to different slices.

255. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

256. The technology claimed in claim 11 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

257. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 19: INFRINGEMENT OF PAT. 7,349,987 CLAIM 15

258. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as

though set forth fully here.

259. Claim 15 of the ’987 Patent provides:

Element A	A method as claimed in claim 10 including a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.

260. IBM directly infringes claim 15 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

261. IBM COS as a Service can optionally encrypt extracted and remainder data prior to storage of the slices by enabling SecureSlice. SecureSlice is independent of the parsing, storing and reconstruction of the data.

262. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

263. The technology claimed in claim 15 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

264. As a direct and proximate result of IBM’s acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 20: INFRINGEMENT OF PAT. 7,349,987 CLAIM 16

265. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

266. Claim 16 of the ’987 Patent provides:

Preamble	A computer readable storage medium encoded with programming instructions for securing data having one or more security sensitive words, characters or icons in a computer system with a plurality physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:
Element A	extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;
Element B	storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and,
Element C	permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

267. IBM directly infringes claim 16 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

268. IBM COS as a Service and IBM COS on premises store data that comprises words, characters, or icons. Some of that data is security sensitive.

269. IBM COS as a Service and IBM COS on premises provide a computer system with a plurality of physically distinguishable memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores.

270. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed herein.

271. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

272. IBM COS as a Service and IBM COS on premises implement security levels for data in multiple ways.

273. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

274. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels (“roles”) of the data (objects and/or buckets).

275. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that

limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

276. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

277. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

278. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. These instructions also enable access to the stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

279. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They enable reconstruction of a full object or a part of an object while providing the appropriate security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

280. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combine the slices including slices with security sensitive content and slices without security sensitive content.

281. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

282. The technology claimed in claim 16 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

283. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 21: INFRINGEMENT OF PAT. 7,349,987 CLAIM 21

284. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

285. Claim 21 of the '987 Patent provides:

Element A	A storage medium with programming instructions as claimed in claim 16 including establishing a plurality of security levels each with a respective security clearance, each said subset of said security sensitive words, characters or icons being correlated with said plurality of security levels and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

286. IBM directly infringes claim 21 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

287. IBM COS as a Service and IBM COS on premises establishes a plurality of security levels. On Information and belief, there are pluralities of these security levels associated with the multiple types of security clearances discussed herein.

288. IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to correlate security clearances to the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

289. IBM COS as a Service and IBM COS on premises divide data into slices. These slices can be retrieved to partially reconstruct the data.

290. IBM COS as a Service and IBM COS on premises support optimizations for partial reads of data, which on information and belief, are employed in at least some instances to permit for a plurality of partial reconstructions.

291. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

292. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific

intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

293. The technology claimed in claim 21 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

294. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 22: INFRINGEMENT OF PAT. 7,349,987 CLAIM 22

295. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

296. Claim 22 of the '987 Patent provides:

Preamble	A computer readable storage medium encoded with programming instructions for securing data with a parsing algorithm via a computer system having physically distinguishable memories designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:
Element A	parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;
Element B	storing said extracted data and said remainder data in said respective extract stores and said remainder store, respectively; and,
Element C	permitting full or partial reconstruction of said data via said extracted data from said respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

297. IBM directly infringes claim 22 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

298. IBM COS as a Service and IBM COS on premises secure data with a parsing algorithm by splitting the data. IBM COS as a Service and IBM COS on premises Accesser nodes split the data using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.”

299. IBM COS as a Service and IBM COS on premises include a plurality of physically distinguishable memories. These memories comprise the various nodes that store slices of customer data. Nodes serve as extract stores and/or remainder stores.

300. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed herein.

301. IBM COS as a Service and IBM COS on premises store data that comprises words, data objects, characters, images, data elements, or icons. Some of that data is security sensitive.

302. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

303. IBM COS as a Service and IBM COS on premises implement security levels for data in multiple ways.

304. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects

and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

305. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

306. Third, IBM COS as a Service and IBM COS on premises use context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

307. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

308. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for parsing the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices with associated security levels but not others.

309. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for storing the sliced data on Slicestor nodes, with

slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance associated with the security level.

310. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They enable reconstruction of a full object or a part of an object while providing the appropriate security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

311. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combines the slices including slices with security sensitive content and slices without security sensitive content.

312. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

313. The technology claimed in claim 22 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

314. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 23: INFRINGEMENT OF PAT. 7,349,987 CLAIM 23

315. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

316. Claim 23 of the ’987 Patent provides:

Element A	A storage medium with programming instructions as claimed in claim 22 wherein the step of parsing parses the data granularly.

317. IBM directly infringes claim 23 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

318. IBM COS as a Service and IBM COS on premises Accesser nodes parse the data using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” The original data is divided on a granular level, sending small subsets of data to different slices.

319. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

320. The technology claimed in claim 23 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

321. As a direct and proximate result of IBM’s acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 24: INFRINGEMENT OF PAT. 7,349,987 CLAIM 27

322. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

323. Claim 27 of the ’987 Patent provides:

Element A	A storage medium as claimed in claim 22 including a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.

324. IBM directly infringes claim 27 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

325. IBM COS as a Service and IBM COS on premises can optionally encrypt extracted and remainder data prior to storage of the slices by enabling SecureSlice. SecureSlice is independent of the parsing, storing and reconstruction of the data.

326. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its

customers to set up and use its systems to operate in an infringing manner.

327. The technology claimed in claim 27 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

328. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 25: INFRINGEMENT OF PAT. 7,552,482 CLAIM 1

329. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

330. Claim 1 of the '482 Patent provides:

Preamble	A method of securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a distributed computer system with a plurality of other computers and a plurality of extract data stores for respective ones of said plurality of security levels, said personal computer, said other computers and said extract data stores operatively connected together over a communications network comprising:
Element A	accepting data input which includes security sensitive content via said personal computer;
Element B	extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;
Element C	storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said personal computer and other computers; and,
Element D	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security

	clearances.

331. IBM directly infringes claim 1 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

332. IBM COS as a Service secures user data stored on a personal computer that comprises words, characters, images, or data objects. Some of that data is security sensitive.

333. IBM COS as a Service stores user data as objects in buckets.

334. IBM COS as a Service implements security levels with predetermined security clearances for data in multiple ways.

335. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

336. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

337. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

338. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

339. IBM COS as a Service operates via a distributed computer system with a plurality of computers and user computers for accessing these nodes. These computers comprise the various nodes that store slices of customer data. Nodes serve as extract stores. On Information and belief, there are pluralities of these extract stores for the security levels discussed above.

340. The IBM COS as a Service system is connected over a communications network.

341. IBM COS as a Service accepts data input via client applications/partner-based interfaces on personal computers when users upload or write data to IBM COS as a Service. Some of that data includes security sensitive content.

342. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

343. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

344. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

345. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

346. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

347. The technology claimed in claim 1 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

348. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 26: INFRINGEMENT OF PAT. 7,552,482 CLAIM 5

349. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

350. Claim 5 of the '482 Patent provides:

Element A	A method as claimed in claim 1 wherein permitting full or partial reconstruction of said data occurs at one of said personal computer and said

	other computers.

351. IBM directly infringes claim 5 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

352. IBM COS as a Service divides data into slices. These slices can be retrieved to reconstruct the data, either fully or partially at the user's personal computer.

353. IBM COS as a Service supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

354. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

355. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

356. The technology claimed in claim 5 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

357. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 27: INFRINGEMENT OF PAT. 7,552,482 CLAIM 25

358. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

359. Claim 25 of the '482 Patent provides:

Element A	A method as claimed in claim 1 wherein extracting occurs either automatically or manually with operator input.

360. IBM directly infringes claim 25 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

361. In IBM COS as a Service, the Accesser nodes extract the security sensitive content automatically when it splits the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

362. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement

and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

363. The technology claimed in claim 25 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

364. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 28: INFRINGEMENT OF PAT. 7,552,482 CLAIM 26

365. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

366. Claim 26 of the '482 Patent provides:

Preamble	A computer readable storage medium containing programming instructions for securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a distributed computer system with a plurality of other computers and a plurality of extract data stores for respective ones of said plurality of security levels, said personal computer, said other computers and said extract data stores operatively connected together over a communications network, the programming instructions comprising:
Element A	accepting data input which includes security sensitive content via said personal computer;
Element B	extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;
Element C	storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of

	said personal computer and other computers; and,
Element D	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

367. IBM directly infringes claim 26 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

368. IBM COS as a Service and IBM COS on premises secure user data stored on a personal computer that comprises words, characters, images, or data objects. Some of that data is security sensitive.

369. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

370. IBM COS as a Service and IBM COS on premises implement security levels with predetermined security clearances for data in multiple ways.

371. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

372. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security

levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

373. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

374. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

375. IBM COS as a Service and IBM COS on premises provide a distributed computer system with a plurality of computers and user computers for accessing these nodes and slicing customer data. Nodes serve as extract stores. These instructions provide for pluralities of these extract stores in IBM COS as a Service and in IBM COS on premises for the security levels associated with the multiple types of security clearances discussed above.

376. The IBM COS as a Service and the IBM COS on premises system is connected over a communications network.

377. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for accepting data input via client applications/partner-based interfaces on personal computers when users upload or write data to IBM COS as a Service or IBM COS on premises. Some of that data includes security sensitive content.

378. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for extracting the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

379. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for storing the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. These instructions provide for accessing stores in IBM COS as a Service and in IBM COS via the corresponding security clearance as discussed previously.

380. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They enable reconstruction of a full object or a part of an object while providing the appropriate security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

381. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combines the slices including slices with security sensitive content and slices without security sensitive content.

382. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent

infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

383. The technology claimed in claim 26 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

384. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 29: INFRINGEMENT OF PAT. 7,552,482 CLAIM 30

385. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

386. Claim 30 of the '482 Patent provides:

Element A	A computer readable storage medium containing programming instructions as claimed in claim 26 wherein permitting full or partial reconstruction of said data occurs at one of said personal computer and said other computers.

387. IBM directly infringes claim 30 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

388. IBM COS as a Service and IBM COS on premises divide data into slices. These slices can be retrieved to reconstruct the data, either fully or partially at the user's personal computer.

389. IBM COS as a Service and IBM COS on premises support optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

390. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

391. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

392. The technology claimed in claim 30 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

393. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 30: INFRINGEMENT OF PAT. 7,552,482 CLAIM 50

394. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

395. Claim 50 of the '482 Patent provides:

Element A	A computer readable storage medium containing programming instructions as claimed in claim 26 wherein extracting occurs either automatically or manually with operator input.

396. IBM directly infringes claim 50 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

397. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for automatically extracting security sensitive content when the Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA). When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

398. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

399. The technology claimed in claim 50 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

400. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 31: INFRINGEMENT OF PAT. 7,721,344 CLAIM 1

401. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

402. Claim 1 of the '344 Patent provides:

Preamble	A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:
Element A	accepting data input which includes security sensitive content via said client computer;
Element B	extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;
Element C	storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said client computer and server computer; and,
Element D	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

403. IBM directly infringes claim 1 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

404. IBM COS as a Service stores data that comprises words, characters, images or data objects. Some of that data is security sensitive.

405. IBM COS as a Service stores user data as objects in buckets.

406. IBM COS as a Service implements security levels with predetermined security clearances for data, including security sensitive content, in multiple ways.

407. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

408. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

409. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

410. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

411. IBM COS as a Service secures data in a client-server computer system with at least one server. This computer system comprises the various nodes that store slices of customer data. Nodes can serve as extract stores.

412. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

413. IBM COS as a Service servers are coupled to client computers and nodes that serve as extract stores.

414. IBM COS as a Service accepts data input via client applications/partner-based interfaces on client computers when users upload or write data to IBM COS as a Service. Some of that data includes security sensitive content.

415. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

416. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

417. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

418. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

419. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object

Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

420. The technology claimed in claim 1 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

421. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 32: INFRINGEMENT OF PAT. 7,721,344 CLAIM 2

422. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

423. Claim 2 of the '344 Patent provides:

Element A	A method as claimed in claim 1 wherein accepting occurs at one of said client computer and said server computer.

424. IBM directly infringes claim 2 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

425. IBM COS as a Service accepts data input via client applications/partner-based interfaces on client computers and the Accesser server computer.

426. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

427. The technology claimed in claim 2 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

428. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 33: INFRINGEMENT OF PAT. 7,721,344 CLAIM 3

429. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

430. Claim 3 of the '344 Patent provides:

Element A	A method as claimed in claim 1 wherein extracting occurs at one of said client computer and said server computer.

431. IBM directly infringes claim 3 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

432. IBM COS as a Service extracts security sensitive content when data is split into slices at the Accesser server computer using an Information Dispersal Algorithm (IDA). When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

433. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

434. The technology claimed in claim 3 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

435. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 34: INFRINGEMENT OF PAT. 7,721,344 CLAIM 4

436. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

437. Claim 4 of the ’344 Patent provides:

Element A	A method as claimed in claim 1 wherein one or both of extracting and storing occurs at said server computer.

438. IBM directly infringes claim 4 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

439. IBM COS as a Service extracts security sensitive content when data is split into slices at the Accesser server computer. IBM COS as a Service stores the slices at the Slicestor server computer.

440. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

441. The technology claimed in claim 4 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

442. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 35: INFRINGEMENT OF PAT. 7,721,344 CLAIM 5

443. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

444. Claim 5 of the '344 Patent provides:

Element A	A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system.

445. IBM directly infringes claim 5 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

446. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

447. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement

and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

448. The technology claimed in claim 5 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

449. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 36: INFRINGEMENT OF PAT. 7,721,344 CLAIM 8

450. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

451. Claim 8 of the '344 Patent provides:

Element A	A method as claimed in claim 1 wherein permitting full or partial reconstruction of said data occurs at one of said client computer and said server computer.

452. IBM directly infringes claim 8 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

453. IBM COS as a Service divides data into slices. These slices can be retrieved to reconstruct the data, either fully or partially, at the Accesser node.

454. IBM COS as a Service supports optimizations for partial reads of data, which on information and belief, are employed in at least some instances.

455. When the client application issues a "read request," the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

456. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

457. The technology claimed in claim 8 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

458. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 37: INFRINGEMENT OF PAT. 7,721,344 CLAIM 16

459. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

460. Claim 16 of the '344 Patent provides:

Element A	A method as claimed in claim 1 wherein storing of said remainder data occurs at one of said server computer and said client computer.

461. IBM directly infringes claim 16 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

462. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

463. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

464. The technology claimed in claim 16 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

465. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 38: INFRINGEMENT OF PAT. 7,721,344 CLAIM 39

466. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

467. Claim 39 of the ’344 Patent provides:

Preamble	A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:
Element A	from input data, extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;
Element B	separately storing said extracted data, for each corresponding security level, in the respective extract store, apart from said remainder data stored in one or both of said client computer and server computer; and,
Element C	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

468. IBM directly infringes claim 39 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

469. IBM COS as a Service stores data that comprises words, characters, images or data objects. Some of that data is security sensitive.

470. IBM COS as a Service stores user data as objects in buckets.

471. IBM COS as a Service implements security levels with predetermined security clearances for data, including security sensitive content, in multiple ways.

472. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security

clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

473. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

474. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

475. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

476. IBM COS as a Service secures data in a client-server computer system with at least one server. This computer system comprises the various nodes that store slices of customer data. Nodes can serve as extract stores.

477. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

478. IBM COS as a Service servers are coupled to client computers and nodes that serve as extract stores.

479. IBM COS as a Service accepts data input via client applications/partner-based interfaces on client computers when users upload or write data to IBM COS as a Service. Some of that data includes security sensitive content.

480. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

481. On Information and belief, slices are stored in a pluralities of extract stores for the security levels associated with the multiple types of security clearances discussed above.

482. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

483. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

484. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

485. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object

Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

486. The technology claimed in claim 39 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

487. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 39: INFRINGEMENT OF PAT. 7,721,344 CLAIM 40

488. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

489. Claim 40 of the '344 Patent provides:

Element A	A method as claimed in claim 39 wherein extracting occurs at one of said client computer and said server computer.

490. IBM directly infringes claim 40 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

491. IBM COS as a Service extracts security sensitive content when data is split into slices at the Accesser server computer using an Information Dispersal Algorithm (IDA). When

the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

492. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

493. The technology claimed in claim 40 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

494. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 40: INFRINGEMENT OF PAT. 7,721,344 CLAIM 41

495. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

496. Claim 41 of the '344 Patent provides:

Element A	A method as claimed in claim 39 wherein one or both of extracting and storing occurs at said server computer.

497. IBM directly infringes claim 41 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

498. IBM COS as a Service extracts security sensitive content when data is split into slices at the Accesser server computer. IBM COS as a Service stores the slices at the Slicestor server computer.

499. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

500. The technology claimed in claim 41 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

501. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 41: INFRINGEMENT OF PAT. 7,721,344 CLAIM 43

502. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as

though set forth fully here.

503. Claim 43 of the ’344 Patent provides:

Element A	A method as claimed in claim 39 wherein said server computer stores said remainder data thereat or in remotely disposed remainder stores in said client-server computer system.

504. IBM directly infringes claim 43 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

505. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

506. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

507. The technology claimed in claim 43 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

508. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 42: INFRINGEMENT OF PAT. 7,721,344 CLAIM 52

509. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

510. Claim 52 of the '344 Patent provides:

Preamble	A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:
Element A	extracting security sensitive content from a data input via said server computer to obtain extracted data for each corresponding security level and remainder data;
Element B	storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,
Element C	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

511. IBM directly infringes claim 52 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

512. IBM COS as a Service stores data that comprises words, characters, images or data objects. Some of that data is security sensitive.

513. IBM COS as a Service stores user data as objects in buckets.

514. IBM COS as a Service implements security levels with predetermined security clearances for data, including security sensitive content, in multiple ways.

515. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

516. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

517. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

518. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

519. IBM COS as a Service secures data in a client-server computer system with at least one server. This computer system comprises the various nodes that store slices of customer data. Nodes can serve as extract stores and a remainder data store.

520. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

521. IBM COS as a Service servers are coupled to client computers and nodes that serve as extract stores.

522. IBM COS as a Service accepts data input via client applications/partner-based interfaces on client computers when users upload or write data to IBM COS as a Service. Some of that data includes security sensitive content.

523. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

524. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

525. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

526. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

527. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

528. The technology claimed in claim 52 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

529. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 43: INFRINGEMENT OF PAT. 7,721,344 CLAIM 53

530. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

531. Claim 53 of the '344 Patent provides:

Element A	A method as claimed in claim 52 wherein said reconstruction is a download operation adapted to be directed at said client computer.

532. IBM directly infringes claim 53 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

533. IBM COS as a Service divides data into slices. The data is reconstructed when the client application issues a “read request,” and the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

534. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

535. The technology claimed in claim 53 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

536. As a direct and proximate result of IBM’s acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 44: INFRINGEMENT OF PAT. 7,721,344 CLAIM 55

537. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

538. Claim 55 of the '344 Patent provides:

Element A	A method as claimed in claim 52 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

539. IBM directly infringes claim 55 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

540. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

541. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

542. The technology claimed in claim 55 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

543. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 45: INFRINGEMENT OF PAT. 7,721,344 CLAIM 79

544. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

545. Claim 79 of the '344 Patent provides:

Preamble	A method of securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels and a remainder data store, said server operatively coupled to at least one client computer and said extract data stores over a communications network comprising:
Element A	facilitating the extraction of security sensitive content from a data input to obtain extracted data for each corresponding security level and remainder data;
Element B	at said server computer, storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in said remainder data store; and,
Element C	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

546. IBM directly infringes claim 79 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

547. IBM COS as a Service stores data that comprises words, characters, images or data objects. Some of that data is security sensitive.

548. IBM COS as a Service stores user data as objects in buckets.

549. IBM COS as a Service implements security levels with predetermined security clearances for data, including security sensitive content, in multiple ways.

550. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

551. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

552. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

553. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

554. IBM COS as a Service secures data in a client-server computer system with at least one server. This computer system comprises the various nodes that store slices of customer data. Nodes can serve as extract stores and remainder data stores.

555. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

556. IBM COS as a Service servers are coupled to client computers and nodes that serve as extract stores.

557. IBM COS as a Service facilitates the extraction of security sensitive content from input data.

558. IBM COS as a Service accepts data input via client applications/partner-based interfaces on client computers when users upload or write data to IBM COS as a Service. Some of that data includes security sensitive content.

559. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

560. IBM COS as a Service stores the sliced data on Slicestor nodes on the Slicestor server computer, with slices with security sensitive content on some nodes and slices without on other nodes. The stores with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

561. IBM COS as a Service permits reconstruction of some or all of the data. It reconstructs a full object or a part of an object. Providing the appropriate security clearance for the security level concerning the data allows retrieval of data from the nodes containing the security sensitive content.

562. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service then combines the slices including slices with security sensitive content and slices without security sensitive content.

563. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

564. The technology claimed in claim 79 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

565. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 46: INFRINGEMENT OF PAT. 7,721,344 CLAIM 80

566. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

567. Claim 80 of the ’344 Patent provides:

Element A	A method as claimed in claim 79 wherein said reconstruction is a download operation adapted to be directed at said client computer.

568. IBM directly infringes claim 80 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

569. IBM COS as a Service divides data into slices. The data is reconstructed when the client application issues a “read request,” and the Accesser node instructs the Slicestor nodes to send the requested data slices for at least part of an object.

570. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

571. The technology claimed in claim 80 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

572. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 47: INFRINGEMENT OF PAT. 7,721,344 CLAIM 82

573. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

574. Claim 82 of the '344 Patent provides:

Element A	A method as claimed in claim 79 wherein said remainder data store is either included in said server computer or is disposed as a separate remainder memory store operatively coupled over said communications network.

575. IBM directly infringes claim 82 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

576. IBM COS as a Service stores the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

577. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users

to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

578. The technology claimed in claim 82 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

579. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 48: INFRINGEMENT OF PAT. 7,721,344 CLAIM 106

580. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

581. Claim 106 of the '344 Patent provides:

Preamble	A computer readable storage medium containing programming instructions for securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a client-server computer system with at least one server computer and a plurality of extract data stores for respective ones of said plurality of security levels, said server operatively coupled to at least one client computer and said extract data stores over a communications network, the programming instructions comprising:
Element A	accepting data input which includes security sensitive content via said client computer;
Element B	extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;
Element C	storing said extracted data for each corresponding security level in the

	respective extract store and storing said remainder data in at least one of said client computer and server computer; and,
Element D	permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

582. IBM directly infringes claim 106 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

583. IBM COS as a Service and IBM COS on premises store data that comprises words, characters, images or data objects. Some of that data is security sensitive.

584. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

585. IBM COS as a Service implements security levels with predetermined security clearances for data, including security sensitive content, in multiple ways.

586. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

587. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security

levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

588. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

589. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

590. IBM COS as a Service and IBM COS on premises provide a distributed computer system with a plurality of computers and user computers for accessing these nodes and slicing customer data. Nodes serve as extract stores. These instructions provide for pluralities of these extract stores in IBM COS as a Service and in IBM COS on premises for the security levels associated with the multiple types of security clearances discussed above.

591. On Information and belief, there are pluralities of these extract stores for the security levels associated with the multiple types of security clearances discussed above.

592. IBM COS as a Service and the IBM COS on premises servers are coupled to client computers and nodes that serve as extract stores.

593. The IBM COS as a Service and the IBM COS on premises system is connected over a communications network.

594. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for accepting data input via client applications/partner-based interfaces on personal computers when users upload or write data to IBM COS as a Service or IBM COS on premises. Some of that data includes security sensitive content.

595. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for extracting the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

596. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for storing the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. These instructions provide for accessing stores in IBM COS as a Service and in IBM COS via the corresponding security clearance as discussed previously.

597. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for reconstructing some or all of the data. They enable reconstruction of a full object or a part of an object while providing the appropriate security clearance for the security level concerning the data to allow for retrieval of data from the nodes containing the security sensitive content.

598. That security clearance may be via ACLs, IAM, or network context as discussed above. IBM COS as a Service and IBM COS on premises then combines the slices including slices with security sensitive content and slices without security sensitive content.

599. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

600. The technology claimed in claim 106 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

601. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 49: INFRINGEMENT OF PAT. 7,721,344 CLAIM 107

602. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

603. Claim 107 of the '344 Patent provides:

Element A	A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer, said client computer and a remainder data store in said client-server computer system.

604. IBM directly infringes claim 107 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM

Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

605. IBM COS as a Service and IBM COS on premises store the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

606. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

607. The technology claimed in claim 107 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

608. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 50: INFRINGEMENT OF PAT. 7,721,344 CLAIM 113

609. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

610. Claim 113 of the '344 Patent provides:

Element A	A computer readable storage medium containing programming instructions as claimed in claim 106 wherein storing of said remainder data occurs at one of said server computer and said client computer.

611. IBM directly infringes claim 113 by setting up and operating IBM Cloud Object Storage as a Service, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

612. IBM COS as a Service and IBM COS on premises store the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

613. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

614. The technology claimed in claim 113 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

615. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 51: INFRINGEMENT OF PAT. 7,958,268 CLAIM 31

616. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

617. Claim 31 of the ’268 Patent provides:

Preamble	A method of securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:
Element A	extracting said security sensitive content from said input data to obtain extracted data for respective security levels;
Element B	facilitating the storage of said extracted data in respective ones of said extract stores; and
Element C	forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

618. IBM directly infringes claim 31 by practicing every step of the claimed method when providing its IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment.

619. IBM COS as a Service secures user data input via a browser. The input data comprises words, characters, images, data elements, or data objects. Some of that data is security sensitive.

620. IBM COS as a Service operates via a distributed computer system. The system comprises various nodes that store slices of customer data. Nodes can serve as extract stores with security levels and clearances as discussed herein.

621. IBM COS as a Service stores user data as objects in buckets.

622. IBM COS as a Service implements security levels with security clearances for data in multiple ways.

623. First, IBM COS as a Service uses access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

624. Second, IBM COS as a Service uses Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

625. Third, IBM COS as a Service uses context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

626. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

627. IBM COS as a Service Accesser nodes split the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

628. IBM COS as a Service facilitates storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The

nodes with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

629. IBM COS as a Service forwards and stores slices of input data without security sensitive content on nodes in the distributed IBM COS system.

630. IBM COS as a Service requires predetermined security clearances to access the extract stores. Providing the appropriate security clearance for the security level concerning the data allows retrieval of and access to data from the nodes containing the security sensitive content.

631. That security clearance may be via ACLs, IAM, or network context as discussed above.

632. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim pursuant to U.S.C. § 271(b) at least by making and/or selling the On-Premises Object Storage deployment options of its Cloud Object Storage product/service. These deployments include IBM hardware appliances or IBM-certified third-party servers with IBM COS software. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

633. The technology claimed in claim 31 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

634. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 52: INFRINGEMENT OF PAT. 7,958,268 CLAIM 36

635. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

636. Claim 36 of the '268 Patent provides:

Preamble	A non-transitory computer readable medium containing programming instructions for securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the programming instructions operably deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:
Element A	extracting said security sensitive content from said input data to obtain extracted data for respective security levels;
Element B	facilitating the storage of said extracted data in respective ones of said extract stores; and
Element C	forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

637. IBM directly infringes claim 36 by setting up and operating IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

638. IBM COS as a Service and IBM COS on premises secure user data input via a browser. The input data comprises words, characters, images, data elements, or data objects. Some of that data is security sensitive.

639. IBM COS as a Service and IBM COS on premises operate via a distributed computer system. The system comprises various nodes that store slices of customer data. Nodes can serve as extract stores with security levels and clearances as discussed herein.

640. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

641. IBM COS as a Service implements security levels with security clearances for data in multiple ways.

642. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

643. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

644. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a

specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

645. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

646. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for splitting the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called “slices.” When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

647. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for facilitating storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes. The nodes with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

648. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for forwarding the sliced data to Slicestor nodes, with slices with security sensitive content stored on some nodes and slices without on other nodes.

649. These instructions enable access, via predetermined security clearances, to the extract stores with security sensitive content. That security clearance may be via ACLs, IAM, or network context as discussed above.

650. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

651. The technology claimed in claim 36 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

652. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 53: INFRINGEMENT OF PAT. 7,958,268 CLAIM 41

653. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

654. Claim 41 of the '268 Patent provides:

Preamble	A non-transitory computer readable medium containing programming instructions for securing data passing through a browser, said data having one or more security sensitive words, characters or icons, used in conjunction with a distributed computer system with a plurality of remote memories respectively designated as corresponding extract stores, each having a respective security level and clearance, comprising:
Element A	extracting said security sensitive words, characters or icons from said data to obtain extracted data for respective security levels and remainder data therefrom;
Element B	facilitating the storage of said extracted data in respective ones of said extract stores; and

Element C	forwarding said remainder data to a targeted destination in said distributed computer system and requiring a respective predetermined security clearance for access to corresponding extract stores.

655. IBM directly infringes claim 41 by setting up and operating IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment, which makes use of computer readable storage media to operate, and also by offering for sale and selling computer readable storage media for implementing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

656. IBM COS as a Service and IBM COS on premises secure user data input via a browser. The input data comprises words, characters, or icons. Some of that data is security sensitive.

657. IBM COS as a Service and IBM COS on premises operate in conjunction with a distributed computer system with a plurality of remote memories. These memories comprise various nodes that store slices of customer data. Nodes can serve as extract stores with security levels and clearances as discussed herein.

658. IBM COS as a Service and IBM COS on premises store user data as objects in buckets.

659. IBM COS as a Service implements security levels with security clearances for data in multiple ways.

660. First, IBM COS as a Service and IBM COS on premises provide access control lists (ACLs) to implement security clearances for the security levels of data in particular objects and buckets. Security clearances for different security levels can be provided via account

universally unique identifiers, email addresses, or groups to provide read/write, read-only, or no-access permissions.

661. Second, IBM COS as a Service and IBM COS on premises provide Identity and Access Management (IAM) policies and roles to implement security clearances for the security levels of data in particular objects and buckets. IAM policies set forth numerous security clearances for differing security levels ("roles") of the data (objects and/or buckets).

662. Third, IBM COS as a Service and IBM COS on premises provide context-based restrictions to implement security clearances for the security levels of data in particular objects and buckets. Security clearances can be provided, for example, via context-based restrictions that limit access to a specific bucket. IBM COS as a Service and IBM COS on premises can secure a specific bucket based upon a security level for that data with a predetermined security clearance for user requests coming from an allowed context, such as a range of IP addressed, VPCs, or service references.

663. On information and belief, these various technologies often operate in conjunction with each other, adding security levels and clearances.

664. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for splitting the data that includes the security sensitive content using an Information Dispersal Algorithm (IDA) to obtain subsets of data called "slices." When the original data includes security sensitive content, that security sensitive content will be found in some slices but not others.

665. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for facilitating storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other

nodes. The nodes with the security sensitive content of a particular security level are accessible via the corresponding security clearance as discussed previously.

666. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for enabling storage of the sliced data on Slicestor nodes, with slices with security sensitive content on some nodes and slices without on other nodes.

667. The computer readable storage media, whether with IBM COS as a Service or IBM COS on premises, include instructions for forwarding the sliced data to Slicestor nodes, with slices with security sensitive content stored on some nodes and slices without on other nodes.

668. These instructions enable access, via predetermined security clearances, to the extract stores with security sensitive content. That security clearance may be via ACLs, IAM, or network context as discussed above.

669. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by actively inducing its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by designing its systems to operate in an infringing manner and encouraging its customers to set up and use its systems to operate in an infringing manner.

670. The technology claimed in claim 41 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

671. As a direct and proximate result of IBM’s acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

COUNT 54: INFRINGEMENT OF PAT. 8,468, 244 CLAIM 1

672. DigitalDoors reasserts and realleges all preceding paragraphs of this Complaint as though set forth fully here.

673. Claim 1 of the ’244 Patent provides:

Preamble	A distributed computer system for organizing and processing data, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat, said plurality of data stores and said server cloud operatively coupled over a communications network, comprising:
Element A	means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud,
Element B	an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;
Element C	a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;
Element D	means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;
Element E	said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.

674. IBM directly infringes claim 1 by making, using, selling, offering for sale, and/or importing IBM Cloud Object Storage as a Service/Public Cloud Object Storage with IBM Cloud deployment and also by making, using, selling, offering for sale, and/or importing its IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage.

675. IBM COS is a distributed computer system that stores and processes data, including select content represented by predetermined words, characters, images, data elements or data objects.

676. The IBM COS system includes a plurality of storage nodes that store customer data. These nodes store slices of data, some of which include data for which heightened security is appropriate.

677. IBM COS storage nodes have access controls and are operatively coupled over a communications network. IBM COS implements access controls for data in multiple ways, including access control lists (ACLs), Identity and Access Management (IAM) policies and roles, and context-based restrictions to for select content data stores and granular data stores.

678. IBM COS nodes identify a plurality of select content data stores for respective ones of a plurality of security designated data in the server cloud.

679. IBM COS nodes extract and store said security designated data in respective select content data stores of said server cloud.

680. IBM COS nodes include a processor that activates at least one of the select content data stores to permit access to the select content data stores and respective security designated data based upon an application of one or more of said access controls thereat. IBM COS nodes allow data to be read from IBM COS based on access controls implemented via ACLs, IAM, and network context as discussed above.

681. IBM COS parses remainder data not extracted from said data to be processed and store the parsed data as data segments in respective granular data stores.

682. IBM COS nodes apply a reconstruction data process employing said respective access controls to combine security designated data and remainder data. That access control may be via ACLs, IAM, or network context as discussed above.

683. Additionally, given its awareness of the patent claim at least after this detailed complaint, IBM is inducing infringement of this claim under 35 U.S.C. § 271(b) by making, importing, using, selling and/or offering for sale IBM Cloud Object Storage on premises via an integrated IBM Solution or as Software Defined Storage, which was designed and intended to practice the system covered by Claim 1 of the '244 Patent. IBM actively induces its customers and end-users to directly infringe every claim limitation with the specific intent to encourage such infringement and knowing that the acts induced constitute patent infringement by encouraging end users to directly infringe the '244 Patent by, as an example, directing and controlling end users' storing of data.

684. The technology claimed in claim 1 was not well understood, routine, or conventional at the time that the application was filed and, by improving computer capabilities, provided a technological solution to a technological problem rooted in computer technology.

685. As a direct and proximate result of IBM's acts of patent infringement, DigitalDoors has been and continues to be injured and has sustained and will continue to sustain damages.

JURY DEMAND

DigitalDoors demands a trial by jury on all issues that may be so tried.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff DigitalDoors requests that this Court enter judgment in its favor and against Defendant as follows:

A. Adjudging, finding, and declaring that IBM has infringed the above-identified claims of each of the Patents-in-Suit under 35 U.S.C. § 271 and that IBM's infringement is willful;

B. Awarding the past and future damages arising out of IBM's infringement of the Patents-in-Suit to DigitalDoors in an amount no less than a reasonable royalty, together with prejudgment and post-judgment interest, in an amount according to proof, and trebling such damages because of the willful nature of IBM's infringement;

C. Adjudging, finding, and declaring that the Patents-in-Suit are valid and enforceable;

D. Awarding attorney's fees, costs, or other damages pursuant to 35 U.S.C. §§ 284 or 285 or as otherwise permitted by law; and

E. Granting DigitalDoors such other further relief as is just and proper, or as the Court deems appropriate, including an accounting of post-verdict infringing sales.

DATED: February 24, 2023

Respectfully submitted,

/s/ *C. Graham Gerst*

C. Graham Gerst
ggerst@giplg.com
Global IP Law Group, LLC

55 W. Monroe St., Ste. 3400
Chicago, Illinois 60603
(312) 241-1500

Melissa R. Smith
(Texas Bar No. 24001351)
GILLAM SMITH LLP
303 South Washington Avenue
Marshall, Texas 75670
Tel: (903) 934-8450
Fax: (903) 934-9257
melissa@gillamsmithlaw.com

Attorneys for Plaintiff DigitalDoors, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system on February 24, 2023.

/s/ *C. Graham Gerst*
C. Graham Gerst