UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
DIVISION

DIGITALDOORS, INC. **4201 COLLINS AVENUE** **SUITE 2103** **MIAMI BEACH, FLORIDA 33140** **Plaintiff**	**CIVIL ACTION:** **8:25-cv- 2**
v.	
SANDY SPRING BANK **17801 GEORGIA AVENUE** **OLNEY, MARYLAND 20832** **Defendant**	

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

DigitalDoors, Inc. ("Plaintiff") hereby files this Original Complaint for Patent Infringement against Defendant, Sandy Spring Bank, and alleges, upon information and belief, as follows:

THE PARTIES

1. DigitalDoors, Inc. is a corporation organized and existing under the laws of the State of Florida with its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, Florida 33140.

2. 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.

3. One aspect of DigitalDoors' data continuity innovation concerns information infrastructure architectures wherein specific data is tagged and distributed for disaster recovery. Such innovation was first described by way of various embodiments in Provisional Applications filed in the United States in 2006 and 2007.

4. Upon information and belief, Defendant is a for-profit corporation organized and existing under the laws of the State ofMaryland, with a principal place of business located at 17801 Georgia Avenue, Olney Maryland 20832. Defendant may be served through its registered agent Daniel J. Schrider, in the State of Maryland at 17801 Georgia Avenue, Olney Maryland 20832. On information and belief, in its extensive role as a consumer and business financial institution (whether Commercial Bank, Thrift, or Credit Union), Sandy Spring Bank makes, uses, sells, offers to sell, and otherwise provides financial account and/or depository services (including but not limited to credit cards, debit cards, checking accounts, savings accounts, and personal and business loans) to consumers throughout the State of Maryland, including in this judicial District, and introduces such services into the stream of commerce knowing and intending that they would be extensively used in the State of Maryland and in this judicial District. Moreover, as an integral component of its services, Sandy Spring Bank is believed to maintain industry standard data backup and disaster recovery systems for the benefit of its customers, including but not limited to Sheltered Harbor Certified systems (*see, e.g.,* https://shelteredharbor.org/) or the functional equivalent thereof. On information and belief, Sandy Spring Bank specifically targets customers in the State of Maryland and in this judicial District.

5. On information and belief, Defendant is a domestically chartered insured "Large Commercial Bank," as classified and reported by the Board of Governors of the Federal Reserve System of the United States. *See www.federalreserve.gov/releases/.* As reported by the Board of Governors in its June 30, 2023 release (*see www.federalreserve.gov/releases/lbr/current/*) (hereafter as "Federal Reserve Report"), Defendant has domestic assets of over One Billion Dollars, and operates domestic branches. On information and belief, such data was obtained by the Federal Reserve from the Consolidated Reports of Condition and Income filed quarterly by the Defendant and from other information in the Board's National Information Center database.

6. On information and belief, Defendant endeavors to provide robust state of the art data security protection to customer financial information, including but not limited to implementing such policies and procedures regarding such protections as dictated by its Board of Directors. According to the Securities and Exchange Commission, it is the responsibility of the Board of Directors to oversee cybersecurity safeguards and ensure the privacy and continuity of client data. *See, e.g.,* Securities and Exchange Commission ("SEC") Compliance Guide entitled: Cybersecurity Risk Management, Strategy, Governance, and incident Disclosure, as modified September 5, 2023, available at: sec.gov/ corpfin/secg-cybersecurity (as visited October 20, 2023) (hereafter as "SEC Article") (discussing SEC Rules relating to cybersecurity, noting that the Rules require, *inter alia*, the annual disclosure of cybersecurity risk management, strategy, and governance, and specifically instructing: "With respect to governance, Item 106 and Item 16K require registrants to describe the board of directors' oversight of risks from cybersecurity threats (including identifying any board committee or subcommittee responsible for such oversight) and management's role in assessing and managing material risks from cybersecurity

threats"). Indeed, SEC Regulation S-K Item 106 (17 CFR § 229.106) expressly requires the following from all registrants in their filings: "Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks." Moreover, Boards of Directors for financial institutions are responsible for safeguarding the customer data managed by the institution, including specifically all account data. *See, e.g.,* FDIC White Paper entitled: Statement Concerning the Responsibilities of Bank Directors and Officers, available at: fdic.gov/regulations/laws/ rules/responsibilities-bank-directors-officers.pdf (as visited October 20, 2023) (hereafter as "FDIC White Paper") (Stating: "Directors and officers of banks have obligations to discharge duties owed to their institution and to the shareholders and creditors of their institutions, and to comply with federal and state statutes, rules and regulations. Similar to the responsibilities owed by directors and officers of all business corporations, these duties include the duties of loyalty and care"); *see also* BankDirector.com Article dated April 14, 2023, entitled: Why the Duty of Cybersecurity is the Next Evolution for Fiduciary Duties, available at: bankdirector.com/committees/governance/ (as visited October 20, 2023) (hereafter as "BankDirector Article") (explaining: "when the duty of oversight meets with the immense cybersecurity responsibilities of financial institutions, a duty of cybersecurity is added to the fiduciary responsibilities of directors and officers," and "Cybersecurity is paramount among the myriad of compliance issues that all corporate officers and directors must address"); *see also* Ernst & Young Article dated June 5, 2023, entitled: The CRO Cyber Risk Agenda: What Boards Should Be Asking, available at: ey.com/en_us/boardmatters/cyber-risk-questions-for-boards (as

visited October 20, 20230 (hereafter as "Ernst & Young Article") (explaining how and why cybersecurity is the top priority for banks and their Boards of Directors). On information and belief, the Board of Directors for the Defendant is fully apprised of Defendant's cybersecurity defense measures, and has fulfilled its duties to its customers by implementing Sheltered Harbor compliant systems and methods.

7. Further on information and belief, Defendant (together with and through its Board of Directors), acts responsibly with respect to cybersecurity. As an integral part of such responsible oversight of customer financial data, and pursuant to its fiduciary duties, Defendant (together with and through its Board of Directors) has implemented Sheltered Harbor compliant systems (or the operational equivalent) to both its production and backup facilities. *See, e.g.,* FFIEC Information Technology Examination Handbook, available at: ithandbook.ffiec.gov/media/2nifgh2b/ffiec_ itbooklet_businesscontinuitymanagement_v3.pdf (as visited October 20, 2023) (hereafter as "FFIEC Handbook"), at 19 and 21.

8. Recognized reports indicate that cyberattacks on enterprises are extremely costly. By way of example, IBM Security estimated that the average cost of a "mega-breach" of more than 50 million records in 2020 was $392 Million, and rising annually. *See* IBM Security Report entitled: Cost of a Data Breach Report 2020, available at: ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf (as visited October 20, 2023) (hereafter as "IBM Report"), at 66-67 (further reporting a cost of $50 Million for a small "megabreach" of only 1 million records); *see also* Dell PowerProtect Cyber Recovery Solution Guide, available at: delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670

-cyber-recovery-sg.pdf (as visited October 20, 2023) (hereafter as "Solution Guide") at 5 (citing report authored by Accenture) (the average cost to an enterprise resulting from a cyberattack is $13 Million). Still further, the 2019 breach of Capital One reportedly resulted in a loss of over $270 Million, in addition to incalculable damage to its goodwill and reputation. *See, e.g.,* TechTarget Article entitled: Paige Thompson Found Guilty in 2019 Capital One Data Breach, available at: techtarget.com/searchsecurity/news/252521775/ (as visited October 20, 2023) (hereafter as "Capital One Article"). As such, financial institutions necessarily devote substantial resources to cyber protections. *See, e.g.,* New York Times Article entitled: Hacking Wall Street, available at: nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html (as visited October 20, 2023) (hereafter as "New York Times Article") (reporting that "[t]he federal government and financial institutions have formed information-sharing groups, performed tabletop exercises and invested heavily in cybersecurity. By estimates and averages, Sandy Spring Bank alone spends about $600 million each year on cybersecurity efforts and has 'more than 3,000 employees' working on the issue in some way").

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this case under 28 U.S.C. §§ 1331 and 1338.

10. This Court has personal jurisdiction over Defendant. Defendant has continuous and systematic business contacts with the State of Maryland. Defendant directly conducts business extensively throughout the State of Maryland, by distributing, making, using, offering for sale, selling, and advertising (including the provision of interactive web pages; the provision and support of payment cards; the provision and support of checking accounts; the provision and

support of secured and unsecured loans; and further including maintaining physical facilities) its services in the State of Maryland and in this District. Defendant has purposefully and voluntarily made its business services, including the infringing systems and services, available to residents of this District and into the stream of commerce with the intention and expectation that they will be purchased and/or used by consumers in this District. On information and belief, Sandy Spring Bank is a provider of: (i) payment cards and card services; (ii) checking and savings account services; and (iii) secured and unsecured loans, throughout the United States. Moreover, as an integral component of its aforementioned services, Sandy Spring Bank is believed to maintain industry standard data backup and disaster recovery systems, including but not limited to Sheltered Harbor Certified systems, within the United States for the benefit of its customers, as well as for regulatory compliance and reputational benefit.

11. On information and belief, Defendant maintains physical brick-and-mortar business locations in the State of Maryland and within this District, retains employees specifically in this District for the purpose of servicing customers in this District, and generates substantial revenues from its business activities in this District. For example, Sandy Spring Bank maintains over fifty business locations in Maryland.

12. On information and belief, Sandy Spring Bank has a substantial presence in the State of Maryland and within this District.

13. On information and belief, Sandy Spring Bank provides a plurality of financial services, including but not limited to providing and supporting payment cards (including but not limited to credit cards, debit cards, and/or prepaid cards) to businesses and individuals located in the State of Maryland and within this District.

14. Further on information and belief, Sandy Spring Bank provides a plurality of financial services, including but not limited to providing and supporting personal and/or business checking and savings accounts, to businesses and individuals located in the State of Maryland and within this District.

15. Further on information and belief, Sandy Spring Bank provides a plurality of financial services, including but not limited to providing and supporting secured and/or unsecured loans (including but not limited to mortgage loans, vehicle loans, personal loans, and/or business loans) to businesses and/or individuals located in the State of Maryland and within this District.

16. Further on information and belief, Sandy Spring Bank maintains control over certain data backup and disaster recovery systems (including, for example, Sheltered Harbor Certified systems) within the United States for the benefit of its customers, as well as for regulatory compliance and reputational benefit.

17. Venue is proper in the District of Maryland as to Defendant pursuant to at least 28 U.S.C. §§ 1391(c)(2) and 1400(b). As noted above, Defendant maintains a regular and established business presence in this District, and specifically targets customers located within this District.

PATENTS-IN-SUIT

18. Plaintiff is the sole and exclusive owner, by assignment, of the following United States Patents: (i) 9,015,301 ("the '301 Patent"); (ii) 9,734,169 ("the '169 Patent"); (iii) 10,182,073 ("the '073 Patent"); and (iv) 10,250,639 ("the '639 Patent") (hereinafter collectively as "the DigitalDoors Patents").

19. By operation of law, the DigitalDoors Patents were originally issued and exclusively vested to the named inventors, Ron M. Redlich and Martin A. Nemzow, as of their respective dates of issuance. *See* 35 U.S.C. § 261; *Schwendimann v. Arkwright Advanced Coating, Inc.,* 959 F.3d 1065, 1072 (Fed. Cir. 2020); *Suppes v. Katti,* 710 Fed. Appx. 883, 887 (Fed. Cir. 2017); *Taylor v. Taylor Made Plastics, Inc.,* 565 Fed. Appx. 888, 889 (Fed. Cir. 2014). Each of Messrs. Redlich and Nemzow, by way of written instruments, assigned all rights, title, and interest in the DigitalDoors Patents to DigitalDoors, Inc. *See* Assignment dated May 5, 2007, as filed with the United States Patent and Trademark Office on June 7, 2007 at Reel 019396 and Frames 0728-0732 (‘301 Patent); *see also* Assignment dated May 27, 2009, as filed with the United States Patent and Trademark Office on May 23, 2013 at Reel 030473 and Frames 0686-0690 (‘169 Patent); *see also* Assignment dated May 5, 2007, as filed with the United States Patent and Trademark Office on June 1, 2021 at Reel 056402 and Frames 0740-0744 (‘073 Patent, and ‘639 Patent). As such, Plaintiff DigitalDoors has sole and exclusive standing to assert the DigitalDoors Patents and to bring these causes of action for infringement and damages.

20. The DigitalDoors Patents are each valid, enforceable, and were each duly issued in full compliance with Title 35 of the United States Code.

21. The inventions described and claimed in the DigitalDoors Patents were invented jointly and exclusively by Ron M. Redlich and Martin A. Nemzow.

22. Joint inventor Ron M. Redlich is a combat veteran of the Israeli military who, in 1974, graduated both Combat Officers School and Air Force Technical Missile Officers School. Mr. Redlich fought in an Air Force Hawk Anti-Aircraft Missile Battery based in Sinai during the 1973 Yom Kippur War. In one instance, the Missile Battery operated by Mr. Redlich was

completely incapacitated for three weeks by Russian Electronic Warfare Weaponry Systems as deployed by the Egyptian military. The electronic attack allowed the Egyptian military to assume full control of the various radar capabilities of the Missile Battery, thus preventing the Battery from launching its protective missiles. As a result, Egyptian bombers were able to attack without resistance, thus inflicting significant damage and many casualties against the Israeli military.

23. Following his military service, Mr. Redlich attended law school at Bar Ilan University in Israel, earning an LLB degree in 1979. Since the tragic events of the Yom Kippur War, Mr. Redlich became determined to develop technological solutions for survivability capabilities against systemic failures. Eventually, the efforts of Mr. Redlich came to fruition in the form of the inventions as described and claimed in the DigitalDoors Patents.

24. The DigitalDoors Patents includes numerous claims defining distinct inventions, and no single claim is representative (for purposes of infringement or validity) of the others. By way of example, Claim 25 of the ’301 Patent recites such steps as “associating at least one data process from a group of data processes,” “applying the associated data process to a further data input,” and multiple options for “activation” of such filters. In contrast, none of Claim 1 of the ’169 Patent, Claim 1 of the ’073 Patent, or Claim 16 of the ’639 Patent include such limitations, Further, Claim 1 of the ’169 Patent recites the “parsing” and “storing” of “remainder data,” whereas Claim 25 of the ’301 Patent does not, nor does Claim 1 of the ’073 Patent. Still further, Claim 1 of the ’073 Patent recites “altering” and “modifying” initially-configured filters, whereas none of Claim 25 of the ’301 Patent, Claim 1 of the ’169 Patent, or Claim 16 of the ’639 Patent include such limitations. Yet still further, Claim 16 of the ’639 Patent recites

"inferencing" of content data, whereas none of Claim 25 of the '301 Patent, Claim 1 of the '169 Patent, or Claim 1 of the '073 Patent include such limitations. These important distinctions are merely representative, as even a cursory review of the claims of the DigitalDoors Patents reveals numerous patentably distinct elements which preclude any single claims from being viewed as representative.

25. The priority date of the DigitalDoors Patents is at least as early as January 5, 2007. As of the priority date, and for at least the reasons set forth herein, the inventions as claimed in the DigitalDoors Patents were novel, non-obvious, unconventional, and non-routine.

26. The DigitalDoors Patents each relate generally to unconventional methods and systems for organizing and processing data in a distributed system and, more particularly, those which extract specific sensitive content for specialized storage and subsequent reconstruction. *See, e.g.,* '301 Patent at Abstract and at 3:17-4:35.

27. As noted, the claims of the DigitalDoors Patents have priority to at least January 5, 2007 (the "Date of Invention"). At that time, the practice of extracting specific content from structured and unstructured data for dedicated disaster recovery to achieve the advantages of the inventions claimed in the DigitalDoors Patents was still many years away. For example, as of the Date of Invention, the conventional approach focused on information recorded in structured data formats with little to no capacity to manage unstructured content. *See, e.g.,* '301 Patent at 1:31-38. Further, and as of the Date of Invention, it was necessary to classify sensitive data, but such was inefficient and inadequate because it did not employ semantic or taxonomic analyses. *See id.* at 1:39-55. Beyond these issues, the state of the art as of the Date of Invention was for enterprises to operate open ecosystems which permitted employees, partners, customers,

vendors, and others to participate in the production of information and the consumption of information. *See id.* at 1:602:3. Such open ecosystems were vulnerable because of the number of access points, thus necessitating robust information rights management functionality. *See id.* at 2:3-27. Still further, as of the Date of Invention, enterprises were largely unable to effectively address the changing sensitivity value of information over the lifecycle of the information file. *See id.* at 2:28-61. In view of the foregoing, there was no convention approach to information management which automatically categorized information in unstructured information files and labeled such information in a way to enable the implementation of policies intended to ensure the proper handling, distribution, retainment, deletion, and management of the information. *See id.* The inventions as described and claimed in the DigitalDoors Patents unconventionally shifted the management approach from data files to the content itself, thus achieving substantial advantages in enterprise information infrastructure management. *See, e.g., id.* at 9:46-58. As such, there is no prior art precursor of any of the extraction engine, select content, categorical filter, contextual filter, conceptual filter, taxonomic filter, adaptive filter, classification engine, mapping system, select data storage architecture, or reconstruction protocol as described in the DigitalDoors Patents.

28. As further evidence of the fact that the inventions as described and claimed in the DigitalDoors patents were unconventional and non-obvious is the known timeline and years-long collective effort on the part of the financial services industry to develop the infringing technologies. More specifically, the financial services industry did not even begin to develop a secure architecture which extracts specific sensitive content for specialized storage and subsequent reconstruction until 2015 as a response to growing cyber threats. *See, e.g.,* Joint

White Paper authored by Dell and Sheltered Harbor entitled: A Sheltered Harbor in a Cyber Storm, available at https://shelteredharbor.org/index.php/about#press (Sheltered Harbor Press Room); also available at: www.delltechnologies.com/asset/en-au/products/data-protection/industry-market/sheltered-harbor-white-paper.pdf (each as visited October 20, 2023) (hereafter as "Joint White Paper"). The fact that the financial services community took several years to develop its own standard is strong evidence that the inventions as claimed in the DigitalDoors Patents were non-obvious, and the fact that the industry did not begin its own development until 2015 is strong evidence that the technological solutions as claimed were unconventional as of the Date of Invention. Indeed, Dell did not fully develop its compliant Sheltered Harbor system until five years after the initialization of the Sheltered Harbor working group. *See, e.g.,* Dell Podcast EP032 (at 2:05-3:20 time mark), available at: www.spreaker.com/user/11960889/power2podcast-ep032 (as visited October 20, 2023) (hereafter as "Dell Podcast"). The fact that Dell spent five years developing its own compliant system is strong evidence that the technical solutions as described and claimed in the DigitalDoors Patents were unconventional and non-obvious as of the Date of Invention. Likewise, the fact that over 900 subject matter experts have contributed to the Sheltered Harbor standards is strong evidence that the technical solutions as described and claimed in the DigitalDoors Patents were unconventional and non-obvious as of the Date of Invention. *See, e.g.,* Cobalt Iron White Paper, entitled: Building Cyber Resilience to Maintain Public Confidence in the Financial Industry: Sheltered Harbor and Cobalt Iron, available at: https://shelteredharbor.org/ index.php/about#press (Press Room); also available at: https://shelteredharbor.org/images/

ShelteredHarbor/Documents/CobaltIron-WhitePaper-SheltredHarbor-20220607_Final.pdf (hereafter as "Cobalt Iron White Paper"). Still further, the fact that the Sheltered Harbor solution is viewed within the technological community as a groundbreaking "blueprint for how modern cyber-protections should be designed and delivered, especially in a very vulnerable industry like financial services" (*see* Dell Podcast (at 4:00-4:25 time mark) is strong evidence that the technical solutions as described and claimed in the DigitalDoors Patents were unconventional and nonobvious as of the Date of Invention. *See also* Cobalt Iron White Paper ("In fact, *now that the financial industry has figured out how to respond to a catastrophic data event*, Sheltered Harbor has formed key alliances to expedite your data vaulting progress").

29. Further, the deficiencies in the state of the art as of the Date of Invention were highly problematic, inasmuch as enterprises could not effectively manage sensitive data at the informational level. *See, e.g.,* '301 Patent at 9:46-58. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering the unconventional approach of implementing categorical filters, including content-based filters, contextual filters, and taxonomic filters, thus allowing substantial data security benefits. As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

30. Still further, in view of the deficiencies in the state of the art as of the Date of Invention, enterprises could not effectively extract specific content from structured and unstructured data. *See, e.g.,* '301 Patent at 1:31-38; 1:50-56; 2:54-61; and 19:53-55. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional taxonomic analysis, including tag placeholder substitution, thus allowing

substantial data security benefits. As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

31. Further, the deficiencies in the state of the art as of the Date of Invention were such that enterprises could not effectively control the security of their open information ecosystems. *See, e.g.,* '301 Patent at 2:3-27. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which includes an inference engine as a counterbalance, thus allowing substantial data security benefits. *See, e.g., id.* at 26:49-27:2. As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

32. As noted, the claims of the DigitalDoors Patents have priority to at least January 5, 2007. The deficiencies in the state of the art as of the Date of Invention were highly problematic, inasmuch as enterprises could not effectively address the changing sensitivity value of information over the lifecycle of the information file. *See id.* at 2:28-61 and 9:53-58. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which includes a life cycle engine, thus allowing substantial security management advantages over an extended period and in view of changing circumstances. *See, e.g., id.* at 26:4927:2. As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

33. Still further, the then-existing dispersal algorithms as of the Date of Invention did

not allow for the mapped dispersal of information to secure and select storage. *See, e.g.,* '301 Patent at 15:23

34. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which includes the ability to disperse content of the whole data stream while maintaining access to the constituent parts of the content. *See id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

35. Likewise, the dispersal algorithms as of the Date of Invention did not allow for the use of granular data which is stored in a known and accessible storage. *See, e.g.,* '301 Patent at 15:43-58. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which reduces security risks by storing smaller and more granular pieces of data, and by modifying the conventional method of allowing access to data only when data is retrieved from a few stores and then combined together. *See id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

36. Further, the conventional systems as of the Date of Invention did not provide a means for performing a first granular extract of data form the source, followed by the use of a dispersal algorithm to secure extracted granular pieces of data, one at a time. *See, e.g.,* '301 Patent at 15:6316:24. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which "brings flexibility to the

system as a whole since granular pieces can be reconstituted, one at a time, and released from [the information dispersal algorithm] for knowledge management operations without compromising the security of the whole document." *See id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance and security over the state of the art.

37. Still further, the conventional systems as of the Date of Invention did not offer the security measures of the inventions as claimed. As described by the inventors: "By securing granular data pieces with the Information Dispersal Algorithm or IDA, the system's granular data parts once reconstituted by the IDA are available in system storage and are stand-alone data structures – (encrypted or not). These stand-alone data structures and the granular data therein can be read on their own without the need to bring together other data shares. Because extracts can be in plain text or decrypted – and stand in their own data structure, the sys-admin can authorize an advanced search and knowledge management operations through the granular data structure." *See* '301 Patent at 16:7-24. These security advances follow from the inventive architecture which, *inter alia*, incorporates filtered and distributed storage. These advantages are explained by the patentee, including as follows: "Distributed storage stores need less security than a centralized data repository for a number of reasons. First, the distributed storage stores hold only parts of the data and they are of lower interest to an attacker that will need to attack few dispersed stores to get the total content. Second, the stores are scattered and if hidden they call for less security. The need for less security means lower costs; more efficiency and less processing power. Thus, dispersal of data to distributed storage stores is inherently 'built in', 'baked in' security." *Id.* at 16:39-47. As such, the technological solutions of the DigitalDoors

Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance and security over the state of the art.

38. Still further, the conventional security protocols as of the Date of Invention were premised on designations permitting access to files beating specific classification labels. *See, e.g.,* '301 Patent at 99:34-65. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional approach which "uses a granular or filter approach to make secure the sensitive data in a particular document. [Select Content] labels, matching the relevancy of the [Select Content] data may be employed rather than security level tags." *Id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

39. The inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to the following: "(a) To automatically control selection of data objects within a data stream and release them in a controlled method only to authorized parties; (b) To automatically separate data objects within a data stream into two or more digital data streams according to the importance and categorization of contents, through extraction and removal of the prioritized content and its replacement by appropriate placeholders; (c) To automatically control selected contents in E-mail, and enable its release in a controlled method only to authorized parties; (d) To enable users to leverage the growth in computer and telecommunications connectivity and electronic commerce by reducing security risks; (e) To enable users to release documents, digital files, and data streams into closed and opened digital networks with the confidence that important, identifying, and critical contents

in that documents, digital files, and data streams is secure and will be seen only by authorized parties; (f) To enable real time simultaneous customization and personalization of selected contents within a data stream to different parties, allowing instant display of the selected content or part of it based on, and tailored made to the status of the user or receiving party; (g) To secure the important and critical contents of a document or digital file by transporting said contents into a separated data stream and removing said data stream to a removed storage memory, while eradicating any copies, temporary caches, or traces of the removed extracts on the original computer or machine; (h) To enable instant return transfer to the display or to another display all or part of extracted content instantly with verification of authorized user; (i) To create a projection of the original document, digital file, data objects within a data stream, or variations of it through combined projection of the splinted data streams, while maintaining separation between the data streams; (j) To create an alternative method for security, instead of encryption, which is secure, cost effective, less timeconsuming, and flexible; (k) To enable automatic timed removal of specific content items, automatically or manually selected from a document, digital file, or data objects within a data stream; [and] (l) To enable an automatic timed reconstruction (reconstitution) of the said document, digital file, or data objects within a data stream." *See, e.g.,* '301 Patent at 102:39103:13. As such, the technological solutions of the DigitalDoors Patents were not well understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

40. The inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to assigning different weights to individual granular content items. *See, e.g.,* '301 Patent at 17:57-18:25. Such enhanced

capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

41. Further, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to improving upon the creation of "tear tagged lines" in the form of contextual ranges within a given data source. *See, e.g.,* '301 Patent at 19:8-49. The inventions unconventionally select ranges of contiguous content and apply an inference engine to assign different weights to different granular content items. *Id.* Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

42. Still further, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to providing a system and method for controlled release of data and granular data streams after verification and validation before the release of each layer. *See, e.g.,* '301 Patent at 20:42-59. The inventions unconventionally reduce security risks by storing smaller and more granular pieces; attackers thus require access to multiple stores to piece together all the content. Further, individual layers of data of the original document data stream may be released at once or at different times. *Id.* Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

43. In addition, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to providing a system and method for flexible content access based on "rolling" granular data exposure with decryption for better workflow. *See, e.g.,* '301 Patent at 21:45-67. The inventions

unconventionally introduce "a solution based on creation of (1) granular pieces of data (2) a distributed storage framework as a way to deal with the need to encrypt yet not overwhelm the processing and other computing workflow. The system creates granular data pieces out of the original document/data stream. This is done through a process of content analysis, selection, extraction and dispersal to distributed storage." *Id.* Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

44. Still further, the conventional security protocols as of the Date of Invention were deficient in their inability to protect privacy and security. *See, e.g.,* '301 Patent at 26:49-27:2. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional approach "by controlling the access to sensitive content. The sensitive information is defined by the inference engine. Documents and data streams are filtered by the inference engine, granular data is selected, (and may be extracted to distributed stores). Granular pieces of data are released by a controlled mechanism to avoid security and privacy breaches." *Id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance, and specifically improved security measures, over the state of the art.

45. Further, the deficiencies in the state of the art as of the Date of Invention were such that search results were imprecise and not comprehensive. *See, e.g.,* '301 Patent at 28:33-47. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional architecture which "establishes an interaction between distributed storage stores with data mining operations." *Id.* As such, and because "searching in

different stores (each one with its own subject matter) results in more robust search results," the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art. *Id.*

46. Still further, the conventional systems as of the Date of Invention failed to store different data extracts in one storage location. *See, e.g.,* '301 Patent at 28:51-29:14. The inventions as claimed in the DigitalDoors Patents overcame the deficiencies in the art by offering an unconventional approach which "stores extracts of a data stream in different memories within one storage location. There is a major difference between splitting a document or a data stream and placing its parts in one storage location and [the inventions as described], which deals with placing extracts of a document or a data stream in one storage location. This invention deals in a situation that a whole data asset was already parsed – and split into a 'remainder' and 'extracts.' What is transferred to one storage location is not all the pieces of a whole document or data assets but partial part of the whole the 'extracts.'" *Id.* As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

47. The inventions of the Asserted Patents unconventionally improve upon online data storage techniques existing as of the Date of invention. As explained by the patentee: "The invention also proposes a new architecture for storage on the internet. The invention enables a user to make as many copies as he wants of a document or data stream with minimal amount of security risk. If a storage node is attacked a small granular piece will not pose a serious threat. A small granular piece does not convey all the substance of the original document/data stream. If

the replicated piece is small enough the attacker will find it useless because it is out of context. For example, a granular piece of data which is a name only can't create a serious threat because it is out of context. Other stores need to be attacked successfully to access their data to give context to the small granular data piece. The security risk of having many copies can be reduced by the user decreasing the size of the granular pieces and dispersing the different pieces to different distributed storage store." *See* '301 Patent at 30:33-57. As such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art.

48. Moreover, the inventions of the Asserted Patents unconventionally improved upon online data storage techniques existing as of the Date of invention by "deliver[ing] capabilities to transform order within the data content into disorder making it very hard for an enemy to attack." *See* '301 Patent at 34:55-35:25. This approach moves away from traditional perimeter security and, as such, the technological solutions of the DigitalDoors Patents were not well-understood, routine, or conventional as of January 2007, and provided greatly improved system performance over the state of the art. *Id.*

49. Still further, the inventions of the Asserted Patents unconventionally improved upon online data storage techniques existing as of the Date of invention by offering an architecture which "minimizes data." More specifically, the inventions "provide a system and method for flexible content access based on rolling granular data exposure with decryption for added security. Granular pieces of the original document/data stream are dispersed to distributed storage nodes to enable a controlled secured environment for release of data. The granular data layers can be exposed one at a time decrypted instead of exposure of a total document." *See* '301

Patent at 35:31-41. As such, the technological solutions of the DigitalDoors Patents were not wellunderstood, routine, or conventional as of January 2007, and provided greatly improved system performance and security over the state of the art. *Id.*

50. In addition, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to "establishing a stronger multilevel security (or MLS) architecture and product, than is currently available." *See, e.g.,* '301 Patent at 98:65-99:14. The inventions unconventionally "introduces multilevel security through sanitization of critical content of a source or plaintext document (or data object) with the unique ability to reconstruct all or part of the original document in conformance to the classification level of the user." *Id.* Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

51. Still further, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to "resolving the major challenges facing government in enabling sharing of information between its different organizations in relationship to conducting military operations as well as fighting terrorism." *See, e.g.,* '301 Patent at 100:41-67. The inventions unconventionally provide an architecture in which granular data is controlled based upon authorization. Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

52. Yet still further, the inventions as described and claimed in the DigitalDoors Patents specifically advance the art in unconventional ways, including but not limited to

"avoiding any one point of failure." *See, e.g.,* '301 Patent at 101:53-102:29. The inventions unconventionally provide an architecture which includes the "creation of substantial lines of defense in depth. The attacker will need to break through many obstacles before accessing all the dispersed data of the document." *Id.* Such enhanced capacity to manipulate granular data unconventionally improved upon the performance and security of data management systems as of the Date of Invention.

53. Still further, as of the Date of Invention, the private sector did not generate or keep the massive amounts of data it now does; not did it have the same concerns about data security or data recovery after a disaster. Likewise, there was very little meaningful private-sector activity directed at addressing these issues. Nevertheless, as of the Date of Invention, the United States government and military collectively generated substantial volumes of data, much of which carried varying levels of secrecy designation. At that time, the government had deficient means of maintaining the secrecy of such data, and external hackers were also a concern. In view of such deficiencies and concerns, and as noted above, Messrs. Redlich and Nemzow founded Digital Doors to develop data-security and survivability solutions for the United States government, and primarily for its military and intelligence agencies. Core features of what DigitalDoors developed included extracting specific content from files, documents, and data objects and then dispersing both the extracted and remainder data separately in pieces to different storage locations. *See, e.g.,* '301 Patent at 16:25-38. This new and inventive method of data extraction and distributed storage increased security because hackers would have to hack multiple locations without knowing where or what they were, or how to fit pieces together. *See, e.g.,* '301 Patent at 16:25-38; 48:56-67. It also provided survivability, particularly

when different copies of the same pieces were distributed in different locations, because a military strike would be unlikely to wipe out all the pieces of the data. *See, e.g.,* '301 Patent at 16:25-38.

54. In view of at least the foregoing, which is merely representative of the disclosures of the DigitalDoors Patents, the claims of the DigitalDoors Patents are not drawn to laws of nature, natural phenomena, or abstract ideas. Although the systems and methods claimed in the DigitalDoors Patents are known and implemented now (and, as a result, are widely infringed), the specific combinations of elements and steps, as recited in the claims, were not conventional or routine as of the Date of Invention.

55. Further, and in view of at least the foregoing, which is merely representative of the disclosures of the DigitalDoors Patents, the claims of the DigitalDoors Patents contain inventive concepts which transform the underlying non-abstract aspects of the claims into patent-eligible subject matter.

56. Consequently, the claims of the DigitalDoors Patents recite methods resulting in improved functionality of the systems on which they are performed and represent technological improvements to the operation of computers as tools of trade.

57. The foregoing facts not only establish a basis to find that the claims of the DigitalDoors Patents were unconventional and non-abstract as of the Date of Invention, they also comprise secondary indicia of non-obviousness.

58. The DigitalDoors Patents were examined by a multitude of United States Patent Examiners, including: Ranodhi Serrao ('301 Patent); Farrukh Hussain ('301 Patent); David Lazaro ('169 Patent); S.M.A. Rahman ('073 Patent and '639 Patent). During the examination of

the DigitalDoors Patents, the United States Patent Examiners searched for prior art in the following US Classifications: 706/59; 707/4; 707/206; 707/609; 707/777; 709/201; 709/203; 709/204; 709/206; 709/217; 709/223; 709/225; 709/226; 707/302; 713/166; 715/748; 726/13; 726/22; 726/23; 726/24; and 726/26.

59. After giving full and proper credit to the prior art and having conducted a thorough search for all relevant art and having fully considered the most relevant art known at the time, the United States Patent Examiners each allowed all of the claims of the DigitalDoors Patents to issue. In so doing, it is presumed that Examiners Serrao, Hussain, Lazaro, and Rahman used their knowledge of the art when examining the claims. *K/S Himpp v. Hear-Wear Techs., LLC,* 751 F.3d 1362, 1369 (Fed. Cir. 2014). It is further presumed that Examiners Serrao, Hussain, Lazaro, and Rahman each had experience in the field of the invention, and that the Examiners properly acted in accordance with a person of ordinary skill. *In re Sang Su Lee,* 277 F.3d 1338, 1345 (Fed. Cir. 2002). In view of the foregoing, the claims of the DigitalDoors Patents are novel and non-obvious, including over all non-cited art which is merely cumulative with the referenced and cited prior art. Likewise, the claims of the DigitalDoors Patents are novel and non-obvious, including over all non-cited contemporaneous state of the art systems and methods, all of which would have been known to a person of ordinary skill in the art, and which were therefore presumptively also known and considered by Examiners Serrao, Hussain, Lazaro, and Rahman.

60. The DigitalDoors Patents are pioneering patents, and have been cited as relevant prior art in hundreds of subsequent United States Patent Applications, including Applications assigned to such technology leaders as Apple, Xerox, Yahoo!, Raytheon, IBM, Mitsubishi,

Blackberry, Microsoft, Dropbox, Oracle, Fujitsu, NEC Corp., Ricoh, Verifone, Google, Sonos, Symantec, Juniper Networks, PriceWaterhouse Coopers, Sony, Amazon, Intuit, Uniloc, Qualcomm, Nokia, Hitachi, Honeywell, Hewlett-Packard, Northrop Grumman, Adobe, State Farm, Facebook, Disney, General Electric, Intel Corp., Siemens, KPMG, Cisco, Equifax, Kyocera, Motorola, Allstate, and Lenovo, in addition to financial services leaders including Wells Fargo, Bank or America, JP Morgan Chase, Capital One, and PayPal.

61. The claims of the DigitalDoors Patents were all properly issued, and are valid and enforceable for the respective terms of their statutory life through expiration, and are enforceable for purposes of seeking damages for past infringement even post-expiration. *See, e.g., Genetics Institute, LLC v. Novartis Vaccines and Diagnostics, Inc.,* 655 F.3d 1291, 1299 (Fed. Cir. 2011) ("[A]n expired patent is not viewed as having 'never existed.' Much to the contrary, a patent does have value beyond its expiration date. For example, an expired patent may form the basis of an action for past damages subject to the six-year limitation under 35 U.S.C. § 286") (internal citations omitted).

62. The nominal expiration date for the claims of the DigitalDoors Patents is no earlier than the year 2028, and as late as the year 2030.

INFRINGING TECHNOLOGIES

63. The financial services industry, as a collective, places great value on the security of customer data. In that regard, "Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting critical account information and data sets of market participants in order to facilitate the recovery and use of such

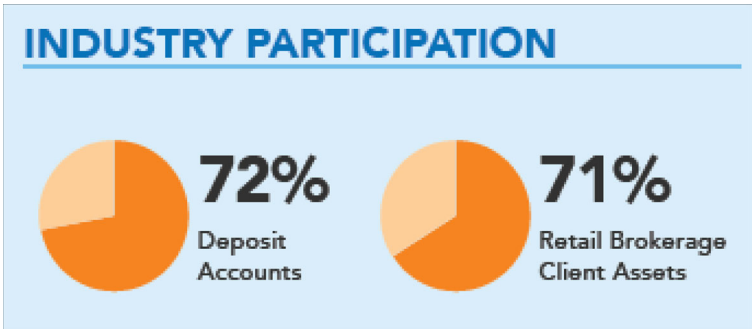
information following a destructive cyberattack or other extreme loss of operational capability. This is achieved through a combination of: (i) *Data Vaulting:* Protection, portability, and recovery standards for critical data sets; (ii) *Resiliency Planning:* Business and technical processes, incident response communications, and key decision arrangements to be activated to ensure continuity of critical customer facing business services when traditional disaster recovery and business continuity plans fail; and (iii) *Certification:* Quality assurance mechanism consisting of requisite controls, processes, independent audits, and management assertions." *See, e.g.,* Sheltered Harbor Operating Rules, January 2023, at § 1.0, available at: https://shelteredharbor.org/images/SH/Docs/Sheltered-Harbor-Operating-Rules.pdf (as visited October 20, 2023) (hereafter as "Operating Rules"). It is widely recognized that "the financial services industry bears a burden of responsibility to be extra diligent in careful planning for protecting customers, recovery against [business disruptions], and providing industry stability." Operating Rules at § 1.0.

64. Sheltered Harbor was founded by 34 financial institutions and is owned by FS-ISAC Inc., which is a nonprofit organization with over 5000 members worldwide. *See* SBS Article entitled "Sheltered Harbor: A Safe Haven From the Perfect Storm," available at: sbscyber.com/resources/ sheltered-harbor-a-safe-haven-from-the-perfect-storm (as visited October 20, 2023) (hereafter as "Safe Haven"); *see also* https://www.fsisac.com/ (About Us) (hereafter as "FS-ISAC Website"). The Board of Directors for FS-ISAC includes representatives from at least the following: (i) Citigroup; (ii) Bank of America; (iii) PNC Bank; (iv) U.S. Bank; (v) Morgan Stanley; (vi) Scotia Bank; (vii) Mass Mutual; (viii) Truist; (ix) Banco Santander; and (x) Deutsche Bank. *See* FSISAC Website. Sheltered Harbor "provides the only

industry-developed standards and certifications for resilience, data recovery, and protection of isolated data." *See* Cobalt Iron White Paper.

65. Sheltered Harbor "coordinates the development of the standards; promotes their adoption across the industry; supports implementation by market participants; and ensures adherence through certification and independent audits. Sheltered Harbor currently supports all financial institutions. With its participant base holding nearly three-quarters of U.S. deposit accounts and retail brokerage assets, Sheltered Harbor is a significant step in the financial sector's ongoing business continuity and operational resilience efforts. Its specifications support the protection of isolated critical data of any type, and its guides support best practices for cyber-resilience preparations." Operating Rules at § 1.0.

66. Stated somewhat differently, it is the express mission of Sheltered Harbor to "protect public confidence in the U.S. financial system if a devastating event like a cyberattack causes an institution's critical systems - including backups - to fail." *See* Sheltered Harbor At-A-Glance, available at: https://shelteredharbor.org/index.php/about#who (Fact Sheet) (as visited October 20, 2023) (hereafter as "At-A-Glance"). Again, there is near uniform participation in the Sheltered Harbor standard across the financial services industry, as reflected in the following graph (*see* AtA-Glance):



67. The Sheltered Harbor initiative "looks to industry experts to define a set of standards that all Sheltered Harbor participants ('Participants') will conform to in order to ensure their firms have the ability to revert to uncompromised data and operationalize this data in a manner that promotes sector stability." Operating Rules at § 1.1.

68. "All Sheltered Harbor's Specifications document the culmination of the work of multiple industry working groups tasked with defining a set of standards that all Sheltered Harbor Participants will conform to in order to protect their critical information and supporting data sets. Sheltered Harbor's Data Protected Specifications describe Participant implementation of the standards for securely storing and recovering critical account data, as well as Participant adherence requirements in the Sheltered Harbor Specifications document. The Data Vaulting Process Specifications describe Participant implementation of the standards for securely storing and recovering selfdefined critical data. Both documents are only available to Sheltered Harbor Participants1. Sheltered Harbor maintains and updates the standards in the Specifications documents through ongoing oversight and adaptation in response to developments in the industry." Operating Rules at § 1.2.

69. The focus of the Sheltered Harbor initiative is to: "(i) Improve resiliency of the U.S. financial system by preventing loss of critical customer account information and supporting data sets; (ii) Establish and maintain commonly agreed data formats and procedures for securely storing and restoring critical financial account data of U.S. Firm Participants to enable restoration and use of such information; (iii) Promote and certify the use of common data formats and procedures for securely storing and restoring critical financial account information;

(iv) When and if necessary, assist in facilitating the recovery of critical customer account data using the Sheltered Harbor procedures and playbooks; and (v) Promote and certify the process for securely storing and restoring self-defined critical data sets." Operating Rules at § 4.1.

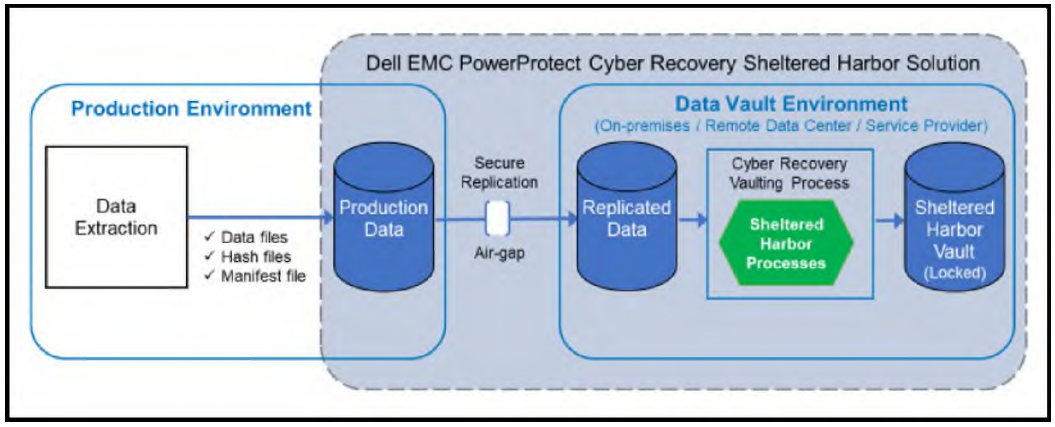
70. One key aspect of the Sheltered Harbor specification is "to create extremely secure (and segmented) backups of financial data across the financial sector." *See* Safe Haven. This objective is accomplished by, *inter alia*, extracting critical financial information from accounts and converting such information into Sheltered Harbor's industry-standard format. The information is then validated, and encryption is applied before the information is transmitted to Sheltered Harbor's secure data vault for storage. Financial institutions who are certified by Sheltered Harbor have the option to store data directly to an in-house data vault which follows Sheltered Harbor's standards, or to otherwise utilize the data vault as an outsourced service. The Sheltered Harbor model assumes there is no central repository for protected accounts. *See* Safe Haven.

71. Under the Sheltered Harbor model, extracted financial information is securely stored until needed by the financial institution. Once needed, the information is transmitted back to the institution as encrypted data to be decrypted. The data then loads back into its core platform and will allow for basic account functions to ensure the institution is able to provide continued service to its customers. *See* Safe Haven.

72. One exemplary system endorsed by Sheltered Harbor (and which satisfies all of the technical requirements established by Sheltered Harbor) is the Dell PowerProtect Cyber Recovery for Sheltered Harbor. *See, e.g.,* Dell Technologies Solution Brief, available at: https://www.delltechnologies.com/asset/en-sg/products/data-protection/briefs-summaries/h18199

-powerprotect-cyber-recovery-for-sheltered-harbor-solution-brief-endorsement.pdf (as visited October 20, 2023) (hereafter as "Dell Sheltered Harbor Solution Brief").

73. As recognized in the Dell Sheltered Harbor Solution Brief, "Sheltered Harbor enhances U.S. financial stability and institutions' cyber resilience by isolating critical customer account records and other data immutably within a digital vault." *See* Dell Sheltered Harbor Solution Brief. The Dell Sheltered Harbor system provides nightly backups of critical data in the Sheltered Harbor standard format, as created by the participating financial institution. The data



vault is encrypted, unchangeable, and isolated from the financial institution's infrastructure. *See id.* The architecture of the Dell Sheltered Harbor system specifically performs the Archive Generation and Secure Repository processes of the Sheltered Harbor standard, as illustrated below (*see* Dell Sheltered Harbor Solution Brief):

74. The Sheltered Harbor specifications require participants to protect critical data sets, including by creating dedicated, isolated environments which are physically separated from corporate networks and backup systems. Such data sets are converted for storage into Sheltered Harbor standardized format so that basic banking services can be quickly resumed for customers

following an attack or failure. *See* Dell Sheltered Harbor Solution Brief.

75. The Dell PowerProtect Cyber Recovery for Sheltered Harbor satisfies all of the technical requirements of the Sheltered Harbor specification, and represents "the culmination of two years of working alongside the Sheltered Harbor team [by Dell] to develop this solution for Financial Services organizations." *See* Dell White Paper entitled: PowerProtect Cyber Recovery Endorsed by Sheltered Harbor, available at https://www.dell.com/en-us/blog/dell-emc-powerprotect-cyber-recovery-endorsed-by-sheltered-harbor/ (as visited October 20, 2023) (hereafter as "Dell Endorsement"). According to the Chief Operating Officer for Sheltered Harbor, the Dell PowerProtect Cyber Recovery system is configured to preserve critical data and ensure rapid recovery "in accordance with Sheltered Harbor's resiliency standards." *See* Dell Endorsement. As similarly stated by Dell, the PowerProtect Cyber Recovery system "meets all of the stringent Sheltered Harbor criteria." *See id.*

76. The Sheltered Harbor specifications are established directly by the financial services industry to ensure that consumers receive timely access to their accounts in the event that their bank becomes inoperable due to a major cyber event. As part of the Sheltered Harbor specification, all participating financial institutions make a daily copy of the consumer's account data in a standard format, which enables the restoration of individual accounts by another institution or processor in the event of a major loss of operations. All participating financial institutions update their adherence reviews to ensure that the Sheltered Harbor standards are exercised consistently and in accordance with Sheltered Harbor specifications. Sensitive account data is archived in a secure data vault that is protected from alteration or deletion. The data

remains intact and accessible if needed, exactly as when it was archived. In this way, each financial institution provides its own data vault. *See* Independent Community Bankers of America article entitled: Operational Risk: Sheltered Harbor, available at: www.icba.org/solutions/operational-risk/cyber-and-data-security/ sheltered-harbor (as visited October 20, 2023) (hereafter as "Operational Risk").

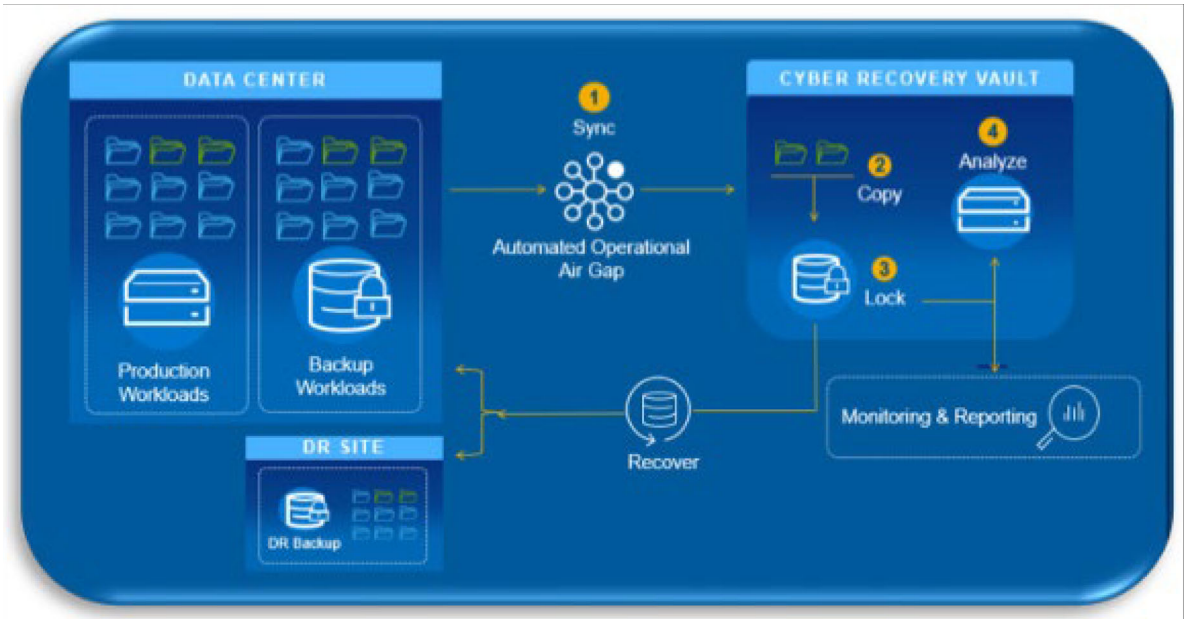
77. The Sheltered Harbor specification identifies a number of critical data vaulting requirements: (i) The vault must be immutable, which means it must be unchangeable and not subject to deletion; The vault must be air-gapped, which means it must be isolated from production and backup systems; (iii) The vault must be survivable and non-accessible, which means it cannot be reliant on infrastructure that can be compromised; (iv) The vault must be decentralized, which means it is not reliant on any single production environment; and (v) The vault must be controlled by the financial institution, which means the data itself is fully owned by the financial institution. *See* Joint White Paper.

78. The Sheltered Harbor specification provides for a common "restoration platform" which includes a standardized set of account data for post-attack restoration and reconstruction. *See* Joint White Paper.

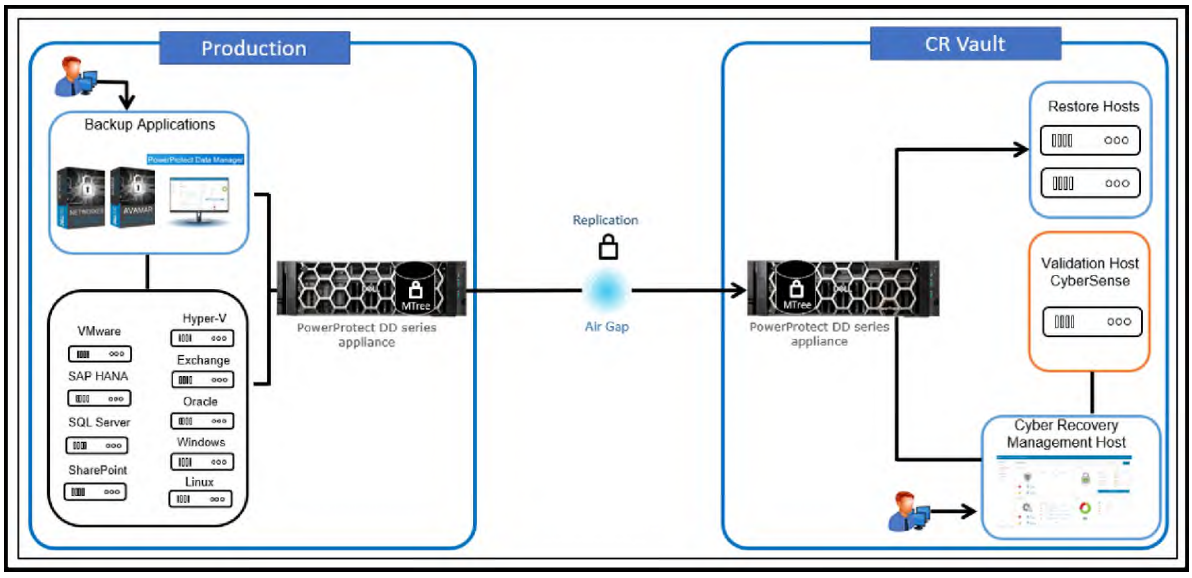
79. As noted, one exemplary system endorsed by Sheltered Harbor (and which satisfies all of the technical requirements established by Sheltered Harbor) is the Dell PowerProtect Cyber Recovery for Sheltered Harbor. The Dell PowerProtect system can be illustrated as follows (*see* Dell Solution Brief entitled: Dell Power Protect Cyber Recovery, available at: www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-

recovery-solution-overview.pdf (as visited October 20, 2023) hereafter as "Dell PowerProtect Solution Brief"):

80. As explained by Dell, "the PowerProtect Cyber Recovery vault offers multiple layers of protection to provide resilience against cyberattacks even from an insider threat. It moves critical data away from the attack surface, physically isolating it within a protected part of the data center and requires separate security credentials and multi-factor authentication for



access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces which could be compromised. PowerProtect Cyber Recovery automates the synchronization of data between production systems including open systems and mainframes, and the vault creating immutable copies with locked retention policies. If a cyberattack occurs you can quickly identify a clean copy of data, recover your critical systems and get your business back up and running." *See* Dell PowerProtect Solution Brief. Post-attack, Dell PowerProtect Cyber Recovery "provides management tools and the



technology that performs the actual data recovery. It automates the creation of the restore points that are used for recovery or security analytics." *See id.*

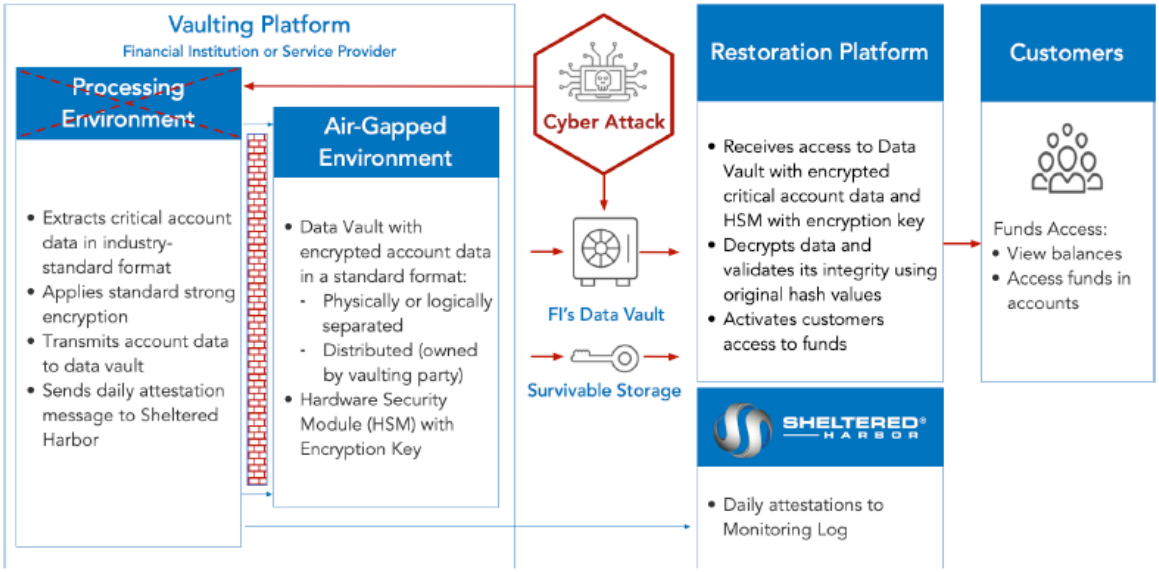
81. The PowerProtect Cyber Recovery vault "is disconnected from the production network through an automated air gap. The vault stores all critical data off-network to isolate it from attack. Cyber Recovery automates data synchronization between production systems and the vault by creating immutable copies with locked retention policies." This system architecture is generally illustrated below. *See* Dell PowerProtect Cyber Recovery: Reference Architecture, available at: www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf (as visited October 20, 2023) (hereafter as "Reference Architecture"):

82. The architecture as illustrated is comprised of two distinct environments: (i) a Production Environment; and (ii) a Vault Environment. With respect to the Production

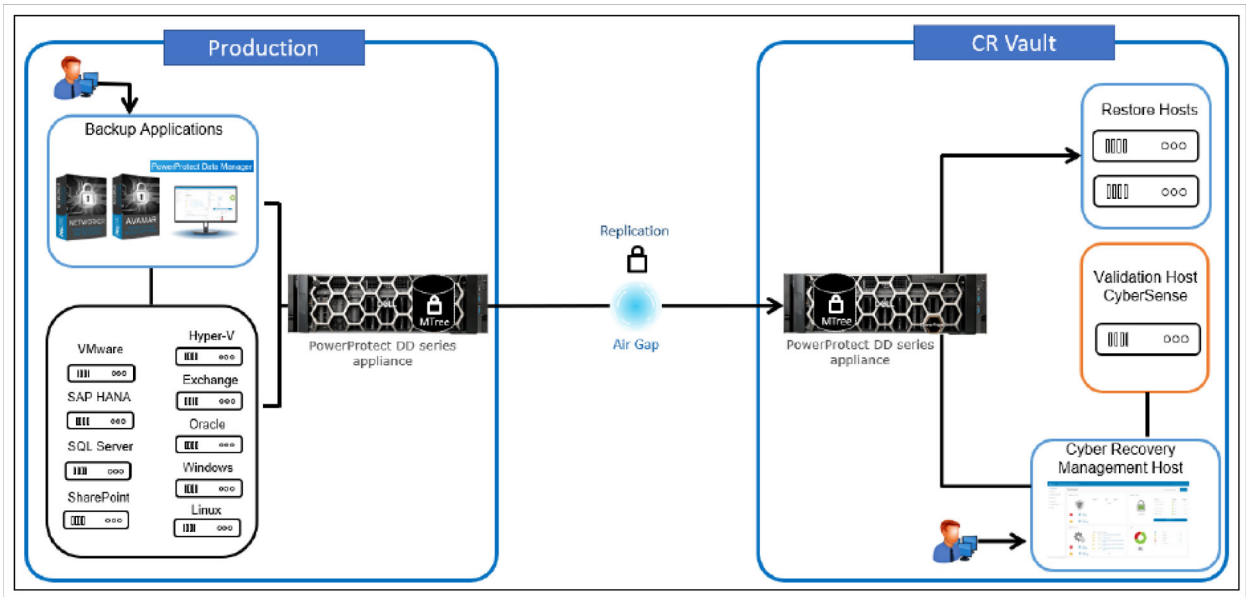
Environment, "it is taken that the data to be protected as part of the Cyber Recovery solution is available in a format supported by the DD series and CyberSense. The data must be stored on a DD series MTree in the production environment." Meanwhile, the Vault Environment "contains a DD series and the Cyber Recovery management host that runs the Cyber Recovery software. Data from the production environment enters the Cyber Recovery vault environment through DD series MTree replication. This environment can also contain various recovery and analytics/indexing physical or virtual hosts that integrate with the solution." *See* Reference Architecture. Further, "server infrastructure is installed in the vault environment and is not shared with or connected to the production environment. Keeping vault server equipment separate from the production environment ensures that any ongoing issues (cyberattacks, operational issues, and so on) do not propagate into the vault environment. Additional safeguards include an automated operational air gap that provides network isolation and eliminates management interfaces." *Id.* Still further, and with respect to the aforementioned "air gap," Dell describes it as follows: "The term 'air gap' implies physical isolation from an unsecure system or network. Logical air gap describes a physical connection but logical isolation from the network. The logical air gap provides another layer of defense by reducing the surface of attack. Cyber Recovery provides the air-gapped feature to keep the Cyber Recovery vault disconnected from the production network. The DD series in the Cyber Recovery vault is disconnected (air-gapped) from the production network most of the time and is only connected when Cyber Recovery triggers replication." *Id.*

83. The Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content in distributed computing systems. *See, e.g.,*

Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id*, at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):



see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:

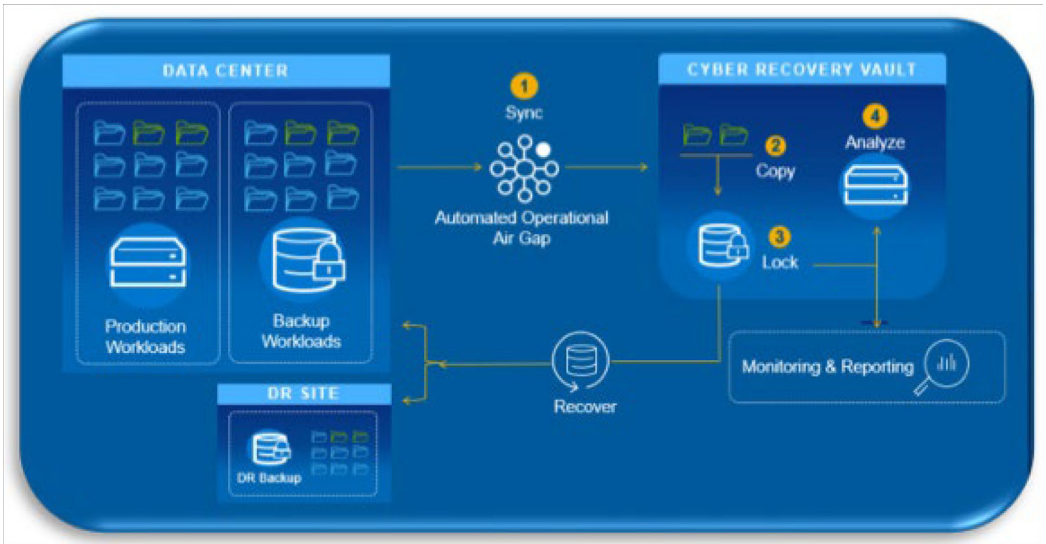


84. The Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability") (italicized emphasis added throughout, unless noted otherwise); *see also* Operating Rules at Exhibit 1 thereof (stating the Processing Environment "Extracts *critical account data* in industry-standard format"); *see also* Dell PowerProtect Cyber Recovery Solution Guide, available at: www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf (as visited October 20, 2023) (hereafter "Solution Guide") at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect any data that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an entire backup application and its backup data, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees").

85. The Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is represented by predetermined words, characters, images, data elements, or objects. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the

recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect *any data* that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an *entire backup application and its backup data*, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees") (and further identifying " *Data, such as application binaries, boot images, and backup catalog*, that must be protected").

86. The Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is stored in a plurality of select content data stores. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. By way of example, and as implemented in compliant systems, the authorized solution from Dell includes a plurality of such data stores, as illustrated below (*see* Dell PowerProtect Solution Brief) (illustrating multiple data stores, including Backup, Copy, Lock, and Analyze):



see also PowerProtect Data Manager Administration and User Guide, available at: www.delltechnologies.com/asset/en-us/products/data-protection/technicalsupport/docu95705.pdf (as visited October 20, 2023) (hereafter as "PowerProtect User Guide") at 52 (stating "When you create a protection policy, the PowerProtect Data Manager software *creates a storage unit on the specified Data Domain backup host* that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*").

87. The Sheltered Harbor standard requires, and is satisfied by, systems in which the data stores for the sensitive content are operative with a plurality of designated categorical filters. As noted, the Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Such data vault is intended to house content derived from designated categorical filters, as established by the enterprise. As explained, the fundamental first step in the Sheltered Harbor process is to: " *Identify the most critical business services that must be protected* and resilient in the face of an 'extreme but plausible event,' and ultimately *map these to the IT data and/or applications necessary to support them*." *See* Joint White Paper. Further, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform ... for those two critical

business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format").

88. As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52.

89. The Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industry-standard format *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, this includes the selection of protection policies by the enterprise, and the selection of conditions for each such policy. *See* PowerProtect Data Manager 19.13, Virtual Machine User Guide, available at: dl.dell.com/

content/manual45487542-powerprotect-data-manager-19-13-virtual-machine-user-guide.pdf?

language=en-us (as visited October 20, 2023) (hereafter as "Virtual Machine User Guide"), at 57. Protection rules are one exemplary embodiment of such categorical filters, which can be implemented in a variety of functionally equivalent ways to achieve the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, "a rule with the filters VM Folder Name, Contains, and Finance can match assets belonging to your finance department to the selected protection policy." *See* Virtual Machine User Guide at 58. The use of such protection rules and attributes for filtering content is a type of categorical filter implementation. *See* Virtual Machine User Guide at 58-59 (detailing use of Protection Rule Attributes, Conditions, Criteria, and Filters (*e.g.,* "contains," "does not contain," "does not equal," "ends with," "equals," "matches RegEx," and "does not match RegEx")).

90. As noted, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Again, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industry-standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, the extracted information is either contextually or taxonomically associated. As explained by the inventors: "A simple classification system (hierarchical taxonomic system) can be established by reviewing the label descriptions on the structured data and then expanding class definitions with the use of the Knowledge Expander (KE) search engine. [...] The hierarchical taxonomic system can be used to build contextual filters and taxonomic filters which can further protect Sec-con data and expand the value and quantity of SC data." *See* '301 Patent

at 10:22-32. In practice, Sheltered Harbor systems allow for the grouping of tags using metadata or any of a number of functionally equivalent means of achieving the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, virtual machine tags are created in the "vSphere Client." Such virtual tags enable the enterprise to attach metadata to virtual inventory assets, making them easier to sort and search. *See* Virtual Machine User Guide at 56. Tags are grouped within categories, which can further include specific object types. *See* Virtual Machine User Guide at 56-58 (describing tag creation and protection rules). The use of tag grouping, including by the use of metadata, is an implementation of contextually or taxonomically associated data.

91. As noted, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such vaulting places aggregated select content into corresponding data stores. The Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. Compliant enterprises further "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. Such "Restoration Platform" understands "a standardized set of data for brokerage or deposit accounts." *See* Joint White Paper. As implemented, compliant systems establish corresponding storage units (or storage trees) in the vault. *See, e.g.,* PowerProtect User Guide at 52; *see also*

Solution Guide at 25 (describing data trees). The aggregated select content can include data, such as binaries, boot images, and backup catalogs. *See, e.g.,* Solution Guide at 25.

92. As noted, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such filtering associates data processes, which include at least one of the following: (i) a copy process (which is linked to a copy data store); (ii) a data extract process (which is linked to an extract store); (iii) a data archive process (which is linked to an archive data store); (iv) a data distribution process (linked to a distribution security level for the select content); and/or (v) a data destruction process. Again, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. The Sheltered Harbor standard further requires enterprises to "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. In so doing, compliant enterprises associate certain data processes with certain select content in order to copy the data to the vault or other data store, extract the data to the vault or other data store, archive the data in accordance with Sheltered Harbor technical requirements, or apply distribution controls on the data in accordance with clearance policies. As implemented, enterprises establish policies which are applied by the compliant Sheltered Harbor system to manage data backup and vaulting. *See*

Virtual Machine User Guide at 38 (explaining backup policy types and levels, including "synthetic-full" and "full" backup). Once a protection policy is established by the enterprise, all further data inputs processed under the filter are processed in the same way. *See, e.g.,* PowerProtect User Guide at 52 ("When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager"). The processing takes place automatically upon a designated time interval (*e.g.,* nightly in accordance with Sheltered Harbor standard), upon a designated condition or event (*e.g.,* upon the detection of new data), or otherwise manually. *See, e.g.,* At-A-Glance ("back up critical customer account data *each night* in the Sheltered Harbor standard format"); *see also* Cobalt Iron White Paper ("Daily attestation messages provide assurance that all backups have been completed and successfully protected"); *see also* PowerProtect User Guide at 145 ("PowerProtect Data Manager *automatically runs dynamic filters* when new assets are detected or when existing assets are modified. You can also run dynamic filters *on demand*").

93. Among other things, the endorsed Dell PowerProtect Cyber Recovery solution complies with, and embodies, the Sheltered Harbor specifications. *See* Reference Architecture (claiming: "Sheltered Harbor endorsement for achieving compliance with financial institution data vaulting standards and certification, planning for operational resilience and recovery, and protecting financial critical data").

94. As an example of another system in development for certification as compliant

with the Sheltered Harbor specifications is the Cobalt Iron and Compass for Sheltered Harbor system. Once developed, the system will be a SaaS platform deployable in either cloud, hybrid, or on-premises options. The Cobalt solution is advertised as being: (i) Secure (encrypted); (ii) Immutable (unchangeable, and not subject to deletion); (iii) Completely isolated from production and backup systems (air-gapped); (iv) Survivable and accessible after a complete system outage; and (v) Under constant role-based access permissions and controls. *See* Cobalt Iron White Paper.

95. Sheltered Harbor compliance can be achieved by an enterprise in one of two ways: (i) use of Sheltered Harbor endorsed technology solution provider (*e.g.,* Cobalt Iron, Dell, FTS, or Veritas) (*see, e.g.,* shelteredharbor.org/index.php/about#howwe); or (ii) independent implementation of the standard (*see, e.g.,* At-A-Glance ("Institutions back up critical customer account data each night in the Sheltered Harbor standard format, *either managing their own vault or using their service provider*"); *see also* Cobalt Iron White Paper ("You are responsible for implementing your own data vault technology and creating your own resiliency plan. However, it's not easy or efficient to develop these solutions from scratch. As you prepare for certification, you don't have to go at it alone. In fact, now that the financial industry has figured out how to respond to a catastrophic data event, Sheltered Harbor has formed key alliances to expedite your data vaulting progress")). In either case, the enterprise itself makes and uses the compliant system, owns all data, and controls the data vault. *See, e.g.,* Joint White Paper (Sheltered Harbor standard requires: "Data fully Owned, and vault Controlled by the financial institution"); *see also* Cobalt Iron White Paper ("The data vault always remains under your control").

96. Sheltered Harbor certification is the industry standard. As explained by Cobalt

Iron: "Acquiring Sheltered Harbor Certification, as recognized by the regulators, is a critical next step financial services organizations (banks, brokerages, etc.) can take toward augmenting their business continuity plans and resilience. Sheltered Harbor Certification signifies that you have implemented the robust set of industry prescribed safeguards and that the prescribed controls have been independently audited for compliance. This ensures public confidence in your institution and the financial system in the worst of scenarios, and that you have a lifeline for survival in an extreme cyber, data corruption or data deletion event." *See* Cobalt Iron White Paper. Further, Sheltered Harbor certification, or its functional equivalent, is required by industry regulations. *See, e.g.,* Cobalt Iron White Paper ("Industry regulation requires that financial institutions prepare for a data destruction event. Participation in Sheltered Harbor demonstrates a proactive approach in planning both a mitigation strategy and a response to a destructive cyberevent. Because Sheltered Harbor started as a public-private partnership that was initiated by regulators, regulators have always been involved in vetting and supporting the solution"); *see also* American Bankers Association commentary entitled: Sheltered Harbor, available at: www.aba.com/banking-topics/technology/ cybersecurity/sheltered-harbor (as visited October 20, 2023) (hereafter as "ABA Article") ("Participating institutions already hold the majority of U.S. deposit accounts and brokerage client assets. To protect the entire industry, 100% participation is optimal," and "We can best protect our customers, ourselves, and the entire U.S. financial system when every financial institution joins").

THE ACCUSED INSTRUMENTALITIES

97. Upon information and belief, Sandy Spring Bank makes, owns, operates, uses, or otherwise exercises control over systems and methods for processing data in a distributed system

which are collectively compliant with the Sheltered Harbor specification. In the alternative, Sandy Spring Bank makes, owns, operates, uses, or otherwise exercises control over systems and methods for processing data in a distributed system which provide substantially equivalent functionality (*i.e.,* providing data backup of critical customer account data to protect against system loss), in a substantially similar way (*i.e.,* by using a plurality of content data stores with categorical filters as described and claimed in the DigitalDoors Patents), to achieve substantially the same results. On information and belief, such methods and systems are implemented by Sandy Spring Bank in the form of a plurality of interconnected storage systems, which are comprised of hardware (including servers) and software (including source code). On information and belief, such hardware and software are made, used, installed, maintained, sold, offered for sale, and tested in the United States on the authority and under the direction or control of Sandy Spring Bank.

98. On information and belief, such data archive systems are directly maintained by, and are accessible to, designated employees and/or representatives of Sandy Spring Bank. Collectively, the foregoing components operate as a single controlled apparatus to provide secure data vaulting for the benefit of Sandy Spring Bank, as specified by Sheltered Harbor or its operational equivalent. Collectively, all of the foregoing comprises the "Accused Instrumentalities."

COUNT I
Infringement of U.S. Patent No. 9,015,301

99. Plaintiff incorporates the above paragraphs by reference.

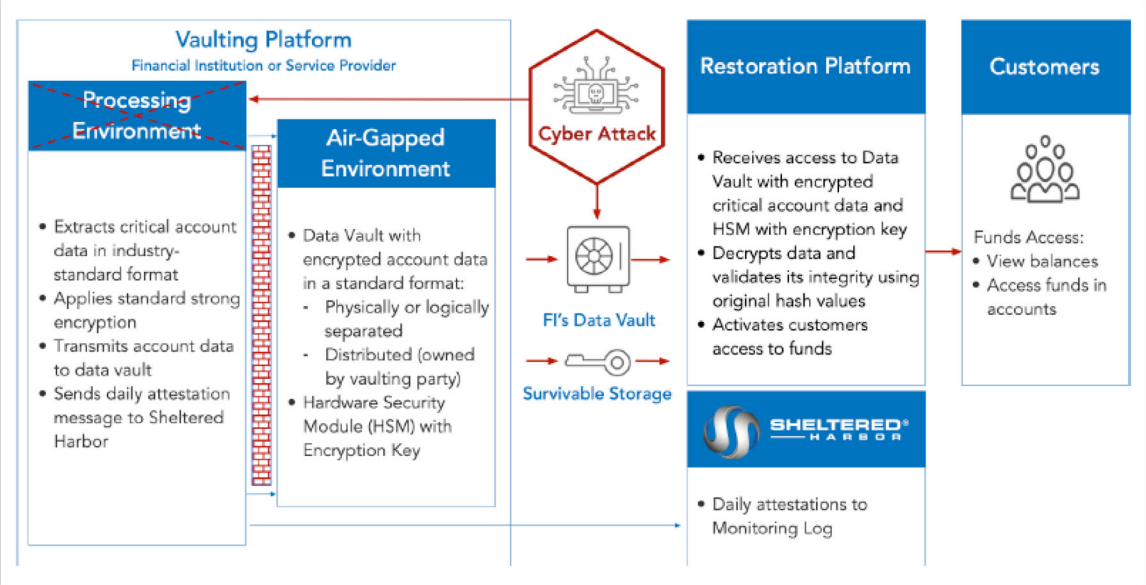
100. Upon information and belief, Defendant owns and/or controls the operation and/or utilization of the Accused Instrumentalities and generates substantial financial revenues therefrom, including but not limited to revenues attributable to business reputation and goodwill, and revenues derived from consumer confidence in the Defendant's ability to protect against cyber threats and maintain operations regardless of external attack or internal system failure.

101. Upon information and belief, Defendant has directly infringed and continues to directly infringe at least Claim 25 of the '301 Patent by making, using, importing, selling, and/or offering for sale the Accused Instrumentalities. The Accused Instrumentalities themselves are specially configured by Defendant to directly perform, and do in fact directly perform, all infringing steps.

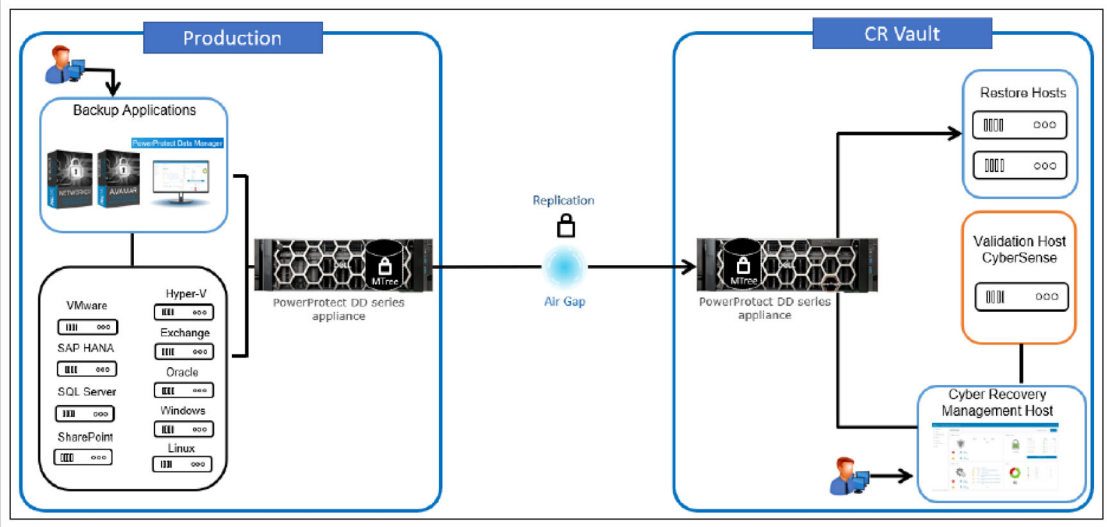
102. Upon information and belief, the Accused Instrumentalities comprise an apparatus which directly performs the claimed method of organizing and processing data in a distributed computing system having select content important to an enterprise operating said distributed computing system and represented by one or more predetermined words, characters, images, data elements or data objects. More specifically, the Accused Instrumentalities comprise a network of servers, hardware, and software for processing data and vaulting such data in compliance with Sheltered Harbor specifications or its operational equivalent, as described herein above. The Defendant is the "enterprise operating the distributed computing system," and Defendant itself makes and uses the system, owns all data, and controls the data vault. *See, e.g.,* Joint White Paper (Sheltered Harbor standard requires: "Data fully Owned, and vault Controlled

by the financial institution"); *see also* Cobalt Iron White Paper ("The data vault always remains under your control"). On information and belief, such apparatus is installed and used in the United States, and such apparatus performs the infringing steps entirely within the United States.

103. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content in distributed computing systems. *See, e.g.,* Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):



see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:



104. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. See, e.g., Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Operating Rules at Exhibit 1 thereof (stating the Processing Environment "Extracts *critical account data* in industry-standard format"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect any data that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an entire backup application and its backup data, the backup software must be able to store both its backup catalog (metadata) and

backup data on one or more PowerProtect DD Mtrees").

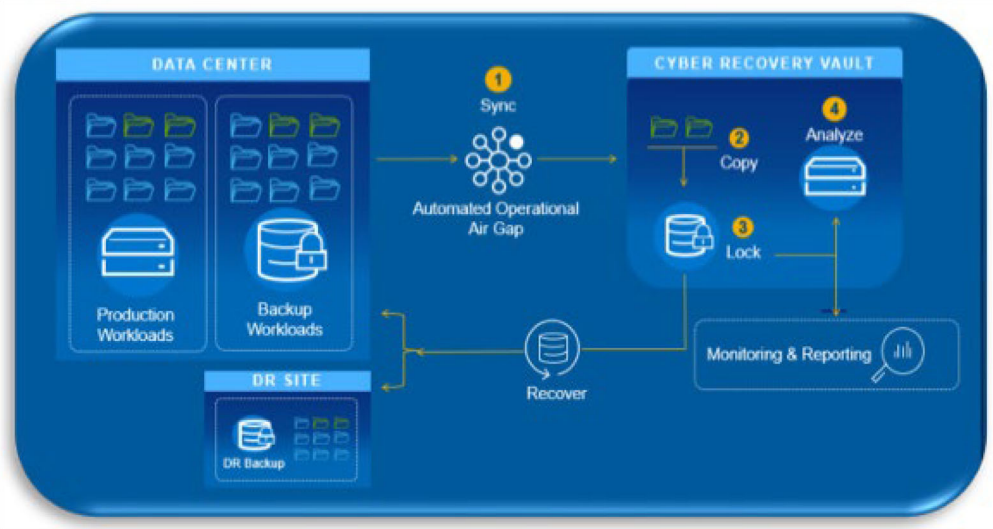
105. Still further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is represented by predetermined words, characters, images, data elements, or objects. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect *any data* that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an *entire backup application and its backup data*, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees") (and further identifying " *Data, such as application binaries, boot images, and backup catalog*, that must be protected").

106. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the claimed method of organizing and processing data in a distributed computing system having select content important to an enterprise operating said distributed computing system and represented by one or more predetermined words, characters, images, data elements or data objects.

107. The Accused Instrumentalities further comprise an apparatus which directly performs the step of providing, in said distributed computing system, a plurality of select content

data stores operative with a plurality of designated categorical filters which stores are operatively coupled over a communications network. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a data vault with designated stores for designated select content, as derived from categorical filters.

108. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is stored in a plurality of select content data stores. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. By way of example, and as implemented in compliant systems, the authorized solution from Dell includes a plurality of such data stores, as illustrated below (*see* Dell PowerProtect Solution Brief) (illustrating multiple data stores, including Backup, Copy, Lock, and Analyze):



see also PowerProtect User Guide at 52 (stating "When you create a protection policy, the PowerProtect Data Manager software *creates a storage unit on the specified Data Domain backup host* that is managed by PowerProtect Data Manager. *All subsequent backups will go to*

this new storage unit").

109. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the data stores for the sensitive content are operative with a plurality of designated categorical filters. As noted, the Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Such data vault is intended to house content derived from designated categorical filters, as established by the enterprise. As explained, the fundamental first step in the Sheltered Harbor process is to: " *Identify the most critical business services that must be protected* and resilient in the face of an 'extreme but plausible event,' and ultimately *map these to the IT data and/or applications necessary to support them*." *See* Joint White Paper. Further, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform ... for those two critical business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration

that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format"). As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52.

110. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of providing, in said distributed computing system, a plurality of select content data stores operative with a plurality of designated categorical filters which stores are operatively coupled over a communications network.

111. The Accused Instrumentalities further comprise an apparatus which directly performs the step of activating at least one of said designated categorical filters and processing a data input therethrough to obtain said select content and associated select content, which associated select content is at least one of contextually associated select content and taxonomically associated select content, as aggregated select content. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which protection policies are implemented using aggregated tags.

112. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain

(extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industry standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, this includes the selection of protection policies by the enterprise, and the selection of conditions for each such policy. *See* Virtual Machine User Guide at 57. Protection rules are one exemplary embodiment of such categorical filters, which can be implemented in a variety of functionally equivalent ways to achieve the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, "a rule with the filters VM Folder Name, Contains, and Finance can match assets belonging to your finance department to the selected protection policy." *See* Virtual Machine User Guide at 58. The use of such protection rules and attributes for filtering content is a type of categorical filter implementation. *See* Virtual Machine User Guide at 58-59 (detailing use of Protection Rule Attributes, Conditions, Criteria, and Filters (*e.g.,* "contains," "does not contain," "does not equal," "ends with," "equals," "matches RegEx," and "does not match RegEx")).

113. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which critical financial account information is extracted and converted into Sheltered Harbor's industry-standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, the extracted information is either contextually or taxonomically associated. As explained by the inventors: "A simple classification system (hierarchical taxonomic system) can be established by reviewing the label descriptions on the structured data and then expanding class definitions with the use of the Knowledge Expander (KE) search engine. [...] The hierarchical taxonomic system can be used to build contextual filters and taxonomic filters which

can further protect Sec-Con data and expand the value and quantity of SC data." *See* '301 Patent at 10:22-32. In practice, Sheltered Harbor systems allow for the grouping of tags using metadata or any of a number of functionally equivalent means of achieving the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, virtual machine tags are created in the "vSphere Client." Such virtual tags enable the enterprise to attach metadata to virtual inventory assets, making them easier to sort and search. *See* Virtual Machine User Guide at 56. Tags are grouped within categories, which can further include specific object types. *See* Virtual Machine User Guide at 56-58 (describing tag creation and protection rules). The use of tag grouping, including by the use of metadata, is an implementation of contextually or taxonomically associated data.

114. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of activating at least one of said designated categorical filters and processing a data input therethrough to obtain said select content and associated select content, which associated select content is at least one of contextually associated select content and taxonomically associated select content, as aggregated select content.

115. The Accused Instrumentalities further comprise an apparatus which directly performs the step of storing said aggregated select content for said at least one categorical filter in said corresponding select content data store. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault stores select content for a designated set of account data, which includes binaries and backups.

116. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such vaulting places aggregated select content into corresponding data stores. The Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. Compliant enterprises further "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. Such "Restoration Platform" understands "a standardized set of data for brokerage or deposit accounts." *See* Joint White Paper. As implemented, compliant systems establish corresponding storage units (or storage trees) in the vault. *See, e.g.,* PowerProtect User Guide at 52; *see also* Solution Guide at 25 (describing data trees). The aggregated select content can include data, such as binaries, boot images, and backup catalogs. *See, e.g.,* Solution Guide at 25.

117. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of storing said aggregated select content for said at least one categorical filter in said corresponding select content data store.

118. The Accused Instrumentalities further comprise an apparatus which directly performs the step of, and for the activated categorical filter, associating at least one data process

from the group of data processes including a copy process, a data extract process, a data archive process, a data distribution process and a data destruction process. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault associates specific actions to specific data types such that the data is copied, archived, extracted, or distributed in accordance with the policies of the enterprise.

119. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such filtering associates data processes, which include at least one of the following: (i) a copy process (which is linked to a copy data store); (ii) a data extract process (which is linked to an extract store); (iii) a data archive process (which is linked to an archive data store); (iv) a data distribution process (linked to a distribution security level for the select content); and/or (v) a data destruction process. Again, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. The Sheltered Harbor standard further requires enterprises to "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. In so doing, compliant enterprises associate certain data processes with certain select content in order to copy the data to the vault or other data store, extract the data to the

vault or other data store, archive the data in accordance with Sheltered Harbor technical requirements, or apply distribution controls on the data in accordance with clearance policies. As implemented, enterprises establish policies which are applied by the compliant Sheltered Harbor system to manage data backup and vaulting. *See* Virtual Machine User Guide at 38 (explaining backup policy types and levels, including "synthetic-full" and "full" backup). Once a protection policy is established by the enterprise, all further data inputs processed under the filter are processed in the same way. *See, e.g.,* PowerProtect User Guide at 52 ("When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager"). The processing takes place automatically upon a designated time interval (*e.g.,* nightly in accordance with Sheltered Harbor standard), upon a designated condition or event (*e.g.,* upon the detection of new data), or otherwise manually. *See, e.g.,* At-A-Glance ("back up critical customer account data *each night* in the Sheltered Harbor standard format"); *see also* Cobalt Iron White Paper ("Daily attestation messages provide assurance that all backups have been completed and successfully protected"); *see also* PowerProtect User Guide at 145 ("PowerProtect Data Manager *automatically runs dynamic filters* when new assets are detected or when existing assets are modified. You can also run dynamic filters *on demand*").

120. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of, and for the

activated categorical filter, associating at least one data process from the group of data processes including a copy process, a data extract process, a data archive process, a data distribution process and a data destruction process.

121. The Accused Instrumentalities further comprise an apparatus which directly performs the step of applying the associated data process to a further data input based upon a result of said further data being processed by said activated categorical filter utilizing said aggregated select content data. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault associates specific actions to specific data types such that the data is copied, archived, extracted, or distributed in accordance with the policies of the enterprise.

122. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such filtering associates data processes, which include at least one of the following: (i) a copy process (which is linked to a copy data store); (ii) a data extract process (which is linked to an extract store); (iii) a data archive process (which is linked to an archive data store); (iv) a data distribution process (linked to a distribution security level for the select content); and/or (v) a data destruction process. Again, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. The Sheltered Harbor standard further requires enterprises to "designate a

restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. In so doing, compliant enterprises associate certain data processes with certain select content in order to copy the data to the vault or other data store, extract the data to the vault or other data store, archive the data in accordance with Sheltered Harbor technical requirements, or apply distribution controls on the data in accordance with clearance policies. As implemented, enterprises establish policies which are applied by the compliant Sheltered Harbor system to manage data backup and vaulting. *See* Virtual Machine User Guide at 38 (explaining backup policy types and levels, including "synthetic-full" and "full" backup).

123. Once a protection policy is established by the enterprise, all further data inputs processed under the filter are processed in the same way. *See, e.g.,* PowerProtect User Guide at 52 ("When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager"). The processing takes place automatically upon a designated time interval (*e.g.,* nightly in accordance with Sheltered Harbor standard), upon a designated condition or event (*e.g.,* upon the detection of new data), or otherwise manually. *See, e.g.,* At-A-Glance ("back up critical customer account data *each night* in the Sheltered Harbor standard format"); *see also* Cobalt Iron White Paper ("Daily attestation messages provide assurance that all backups have been completed and successfully protected"); *see also* PowerProtect User Guide at 145 ("PowerProtect Data Manager

automatically runs dynamic filters when new assets are detected or when existing assets are modified. You can also run dynamic filters *on demand*").

124. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of applying the associated data process to a further data input based upon a result of said further data being processed by said activated categorical filter utilizing said aggregated select content data.

125. The Accused Instrumentalities further comprise an apparatus which directly performs the step of activating a designated categorical filter, which encompasses an automatic activation or a manual activation and said automatic activation is time-based, distributed computer system conditionbased, or event-based. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault associates specific actions to specific data types such that the data is copied, archived, extracted, or distributed in accordance with the policies of the enterprise.

126. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such filtering associates data processes, which include at least one of the following: (i) a copy process (which is linked to a copy data store); (ii) a data extract process (which is linked to an extract store); (iii) a data archive process (which is linked to an archive data store); (iv) a data distribution process (linked to a distribution security level for the select content); and/or (v) a data destruction process. Again, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in

the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. The Sheltered Harbor standard further requires enterprises to "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. In so doing, compliant enterprises associate certain data processes with certain select content in order to copy the data to the vault or other data store, extract the data to the vault or other data store, archive the data in accordance with Sheltered Harbor technical requirements, or apply distribution controls on the data in accordance with clearance policies. As implemented, enterprises establish policies which are applied by the compliant Sheltered Harbor system to manage data backup and vaulting. *See* Virtual Machine User Guide at 38 (explaining backup policy types and levels, including "synthetic-full" and "full" backup). Once a protection policy is established by the enterprise, all further data inputs processed under the filter are processed in the same way. *See, e.g.,* PowerProtect User Guide at 52 ("When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager"). The processing takes place automatically upon a designated time interval (*e.g.,* nightly in accordance with Sheltered Harbor standard), upon a designated condition or event (*e.g.,* upon the detection of new data), or

otherwise manually. *See, e.g.,* At-A-Glance ("back up critical customer account data *each night* in the Sheltered Harbor standard format"); *see also* Cobalt Iron White Paper ("Daily attestation messages provide assurance that all backups have been completed and successfully protected"); *see also* PowerProtect User Guide at 145 ("PowerProtect Data Manager *automatically runs dynamic filters* when new assets are detected or when existing assets are modified. You can also run dynamic filters *on demand*").

127. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of activating a designated categorical filter, which encompasses an automatic activation or a manual activation and said automatic activation is time-based, distributed computer system condition-based, or event-based.

128. The foregoing infringement on the part of Defendant has caused past and ongoing injury to Plaintiff. The amount of damages adequate to compensate for the infringement shall be determined at trial but is in no event less than a reasonable royalty from the date of first infringement to the expiration of the '301 Patent.

129. To the extent Defendant continues, and has continued, its infringing activities noted above in an infringing manner post-notice of the '301 Patent, such infringement is necessarily willful and deliberate.

Each of Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

COUNT II
Infringement of U.S. Patent No. 9,734,169

130. Plaintiff incorporates the above paragraphs by reference.

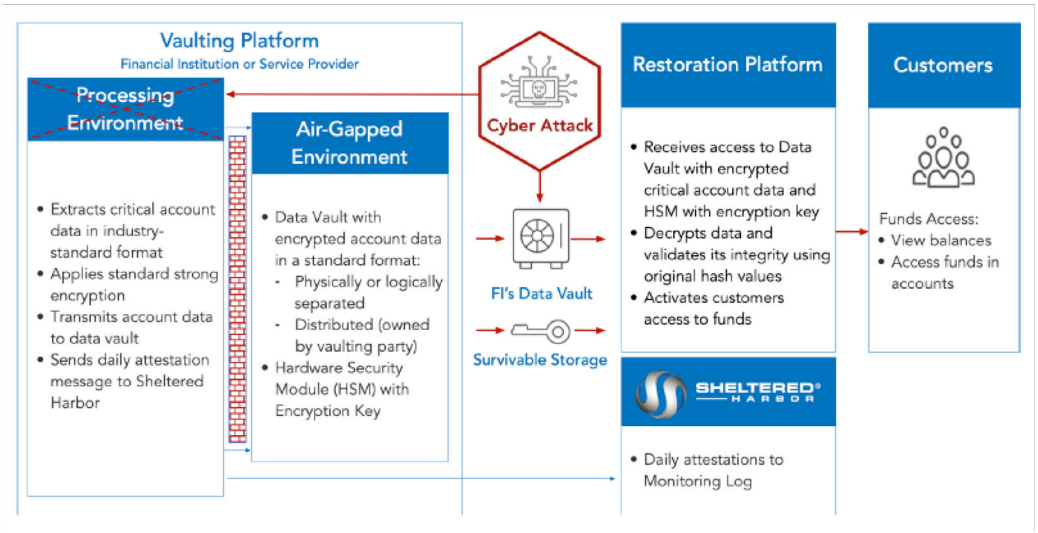
131. Upon information and belief, Defendant owns and/or controls the operation and/or utilization of the Accused Instrumentalities and generates substantial financial revenues therefrom, including but not limited to revenues attributable to business reputation and goodwill, and revenues derived from consumer confidence in the Defendant's ability to protect against cyber threats and maintain operations regardless of external attack or internal system failure.

132. Upon information and belief, Defendant has directly infringed and continues to directly infringe at least Claim 1 of the '169 Patent by making, using, importing, selling, and/or offering for sale the Accused Instrumentalities. The Accused Instrumentalities themselves are specially configured by Defendant to directly perform, and do in fact directly perform, all infringing steps.

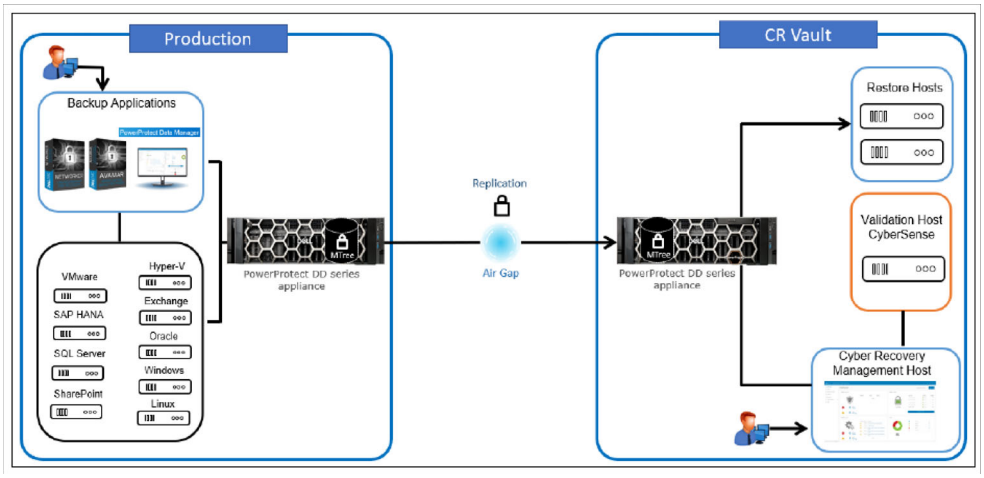
133. Upon information and belief, the Accused Instrumentalities comprise an apparatus which directly performs the claimed method of organizing and processing data in a distributed cloud-based computing system having select content represented by one or more predetermined words, characters, images, data elements or data objects. More specifically, the Accused Instrumentalities comprise a cloud-based network of servers, hardware, and software for processing data and vaulting such data in compliance with Sheltered Harbor specifications or its operational equivalent, as described herein above. The Defendant is the "enterprise operating the distributed computing system," and Defendant itself makes and uses the system, owns all data, and controls the data vault. *See, e.g.,* Joint White Paper (Sheltered Harbor standard requires: "Data fully Owned, and vault Controlled by the financial institution"); *see also* Cobalt Iron White Paper ("The data vault always remains under your control"). On information and belief, such apparatus is installed and used in the United States, and such apparatus performs the

infringing steps entirely within the United States.

134. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content in distributed computing systems. See, e.g., Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):



see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:



135. Still further, and on information and belief, such systems as implemented by Defendant are cloud-based. By way of example, the Accused Instrumentalities are optionally implemented on Amazon Web Services Cloud, Google Cloud, IBM Enterprise Cloud, Rackspace Cloud, Microsoft Cloud (Azure), DigitalOcean, Dell Cloud (Apex). or an alternative functional equivalent thereof. As implemented in compliant systems, the authorized solution from Dell is designed and intended for deployment on any of Amazon Web Services, Microsoft Azure, and Google Cloud. *See, e.g.,* Solution Guide at 31; *see also* Cobalt Iron White Paper (describing cloud solution, and noting that its Compass Solution "enables enterprises to transform and optimize legacy backup solutions into a simple cloud-based architecture with built-in cybersecurity").

136. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Operating Rules at Exhibit 1 thereof (stating the Processing Environment "Extracts *critical account data* in industry-standard format"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect any data that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an entire backup application and its

backup data, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD Mtrees").

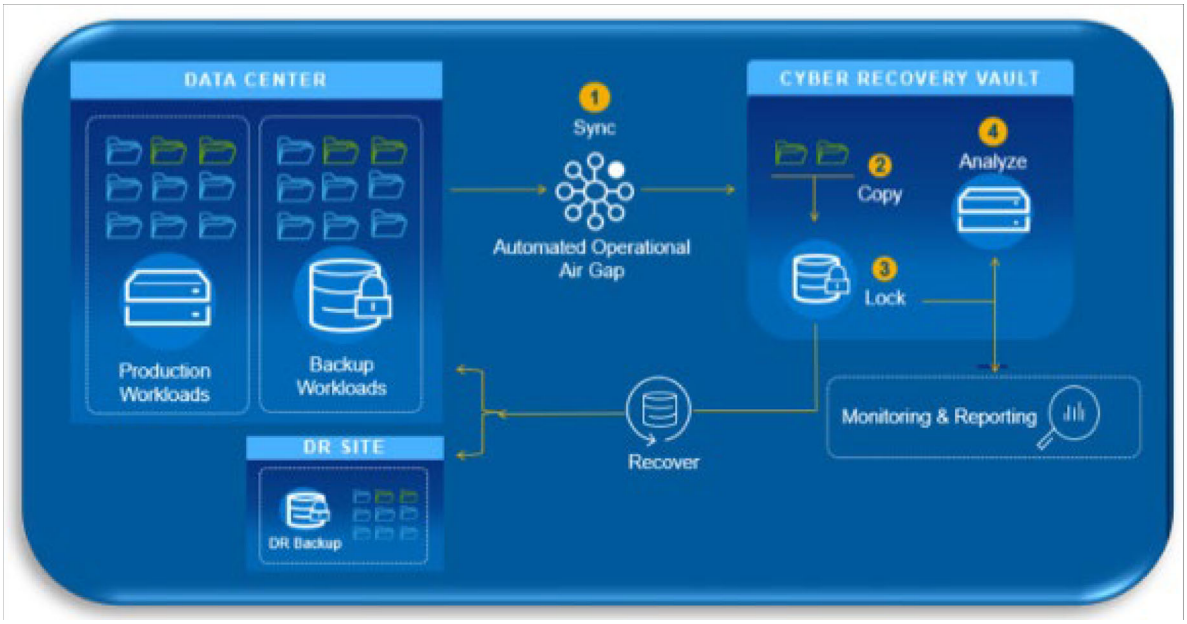
137. Still further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is represented by predetermined words, characters, images, data elements, or objects. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect *any data* that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an *entire backup application and its backup data*, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees") (and further identifying " *Data, such as application binaries, boot images, and backup catalog*, that must be protected").

138 In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the claimed method of organizing and processing data in a distributed cloud-based computing system having select content represented by one or more predetermined words, characters, images, data elements or data objects.

139. The Accused Instrumentalities further comprise an apparatus which directly

performs the step of providing in said distributed cloud-based computing system: (i) a plurality of select content data stores for respective ones of a plurality of security designated data; and (ii) a plurality of granular data stores; and (iii) a cloud-based server, each select content data store having respective access controls thereat. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a data vault with designated stores for designated select content, as derived from categorical filters.

140. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is stored in a plurality of select content data stores. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. By way of example, and as implemented in compliant systems, the authorized solution from Dell includes a plurality of such data stores, as illustrated below (*see* Dell PowerProtect Solution Brief) (illustrating multiple data



stores, including Backup, Copy, Lock, and Analyze):

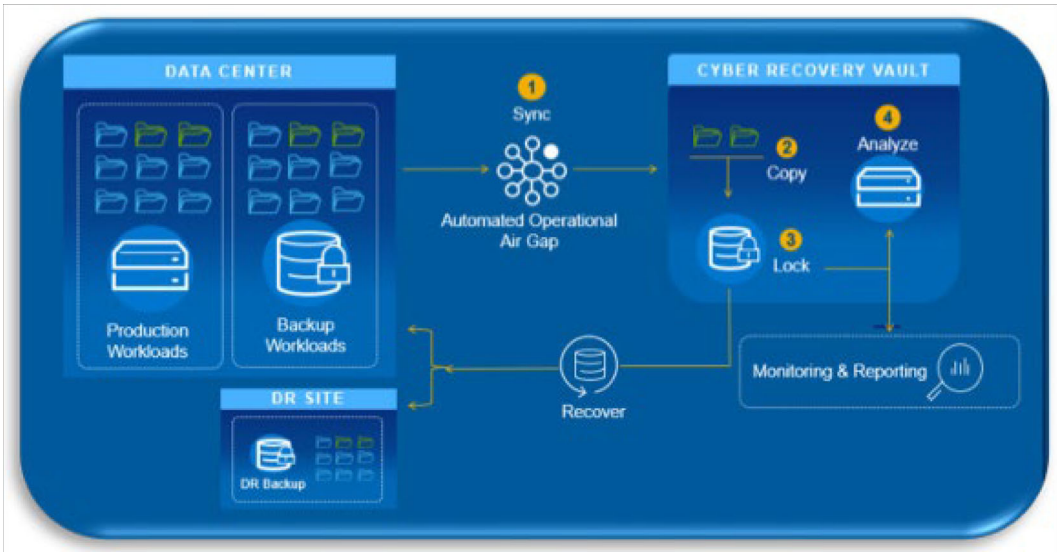
see also PowerProtect User Guide at 52 (stating "When you create a protection policy, the PowerProtect Data Manager software *creates a storage unit on the specified Data Domain backup host* that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*").

141. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the data stores for the sensitive content are operative with a plurality of designated categorical filters. As noted, the Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Such data vault is intended to house content derived from designated categorical filters, as established by the enterprise. As explained, the fundamental first step in the Sheltered Harbor process is to: " *Identify the most critical business services that must be protected* and resilient in the face of an 'extreme but plausible event,' and ultimately *map these to the IT data and/or applications necessary to support them*." *See* Joint White Paper. Further, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform ... for those two critical business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to

provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format"). As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52. Of course, each data store includes access controls, as implemented via security credentials and/or multi-factor authentication, or a functional equivalent. *See, e.g.,* Solution Guide at 21-22 (describing data access protocols).

142. Still further, the Sheltered Harbor standard requires, and is satisfied by, systems in which a plurality of granular data stores are implemented. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Additionally, the data vault is required by Sheltered Harbor as being "air-gapped," or "isolated from production and backup systems." *See* Joint White Paper. As implemented in compliant systems, the authorized solution from Dell is designed and intended for deployment in an "air-gapped" architecture which is isolated from the production backup system (which itself serves as a plurality of granular data stores). *See, e.g.,* Enterprise Strategy Group White Paper entitled: Protecting Critical Data from Cyber Threats Such as Ransomware

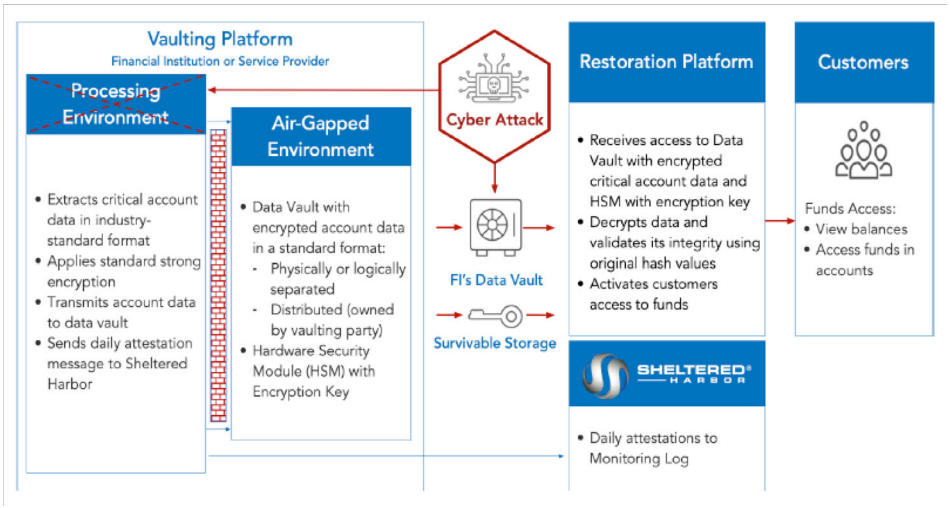
with a Comprehensive Digital Vault Solution, available at: delltechnologies.com/asset/en-us/products/data-protection/industry-market/esg-cyber-recovery-tech-validation-report.pdf (as visited October 20, 2023) (hereafter as "Dell Digital Vault Solution"), at 7 (describing process of pulling data from backup storage on the production side); *see also* Dell PowerProtect Solution Brief (illustrating multiple granular data stores as "Backup Workloads"), as reproduced below:



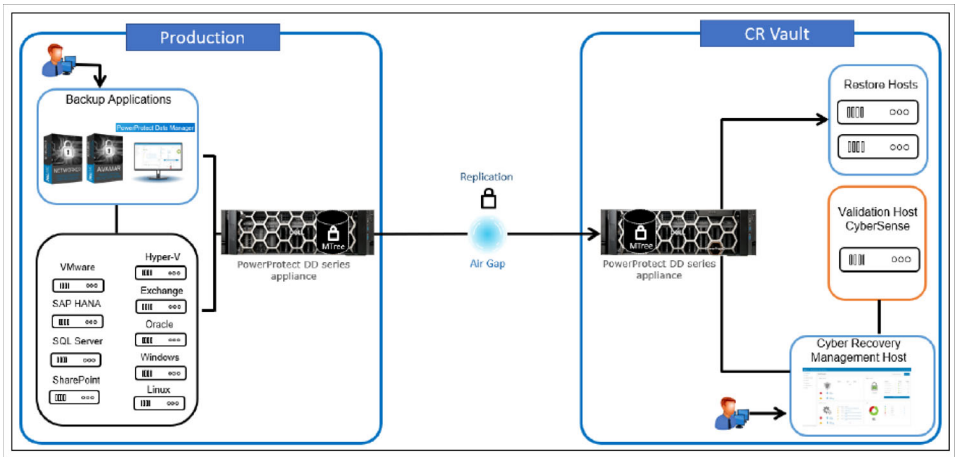
143. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of providing in said distributed cloudbased computing system: (i) a plurality of select content data stores for respective ones of a plurality of security designated data; and (ii) a plurality of granular data stores; and (iii) a cloud based server, each select content data store having respective access controls thereat.

144. The Accused Instrumentalities further comprise an apparatus which directly performs the step of providing a communications network operatively coupling said plurality of

select content data stores and cloud-based server. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a distributed, cloud-based system which is configured to manage and protect data containing sensitive content. *See, e.g.,* Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):



see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:



145. Still further, and on information and belief, such systems as implemented by Defendant are cloud based (as discussed in detail above), and necessarily comprise an operatively coupled communications network. *See, e.g.,* Dell Digital Vault Solution at 7 (describing network with dedicated interfaces); *see also* At-A-Glance (data vault is required to be "completely separated" from the infrastructure of the compliant enterprise; also describing the "restoration platform"); *see also* Joint White Paper (Sheltered Harbor requires data vault to be both "survivable" and "accessible").

146. The Accused Instrumentalities comprise an apparatus which directly performs the step of (with respect to data processed by said cloud-based system) extracting and storing said security designated data in respective select content data stores. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which protection policies are implemented using aggregated tags.

147. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industry standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, this includes the selection of protection policies by the enterprise, and the selection of conditions for each such policy. *See* Virtual Machine User Guide at 57. Protection rules are one exemplary embodiment of such categorical filters, which can be implemented in a variety of functionally equivalent ways to achieve the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system,

"a rule with the filters VM Folder Name, Contains, and Finance can match assets belonging to your finance department to the selected protection policy." *See* Virtual Machine User Guide at 58. The use of such protection rules and attributes for filtering content is a type of categorical filter implementation. *See* Virtual Machine User Guide at 58-59 (detailing use of Protection Rule Attributes, Conditions, Criteria, and Filters (*e.g.,* "contains," "does not contain," "does not equal," "ends with," "equals," "matches RegEx," and "does not match RegEx")).

148. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which critical financial account information is extracted and converted into Sheltered Harbor's industry-standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, the extracted information is either contextually or taxonomically associated. As explained by the inventors: "A simple classification system (hierarchical taxonomic system) can be established by reviewing the label descriptions on the structured data and then expanding class definitions with the use of the Knowledge Expander (KE) search engine. [...] The hierarchical taxonomic system can be used to build contextual filters and taxonomic filters which can further protect Sec-Con data and expand the value and quantity of SC data." *See* '301 Patent at 10:22-32. In practice, Sheltered Harbor systems allow for the grouping of tags using metadata or any of a number of functionally equivalent means of achieving the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, virtual machine tags are created in the "vSphere Client." Such virtual tags enable the enterprise to attach metadata to virtual inventory assets, making them easier to sort and search. *See* Virtual Machine User Guide at 56. Tags are grouped within categories, which can further include specific object types. *See* Virtual Machine User Guide at 56-58 (describing

tag creation and protection rules). The use of tag grouping, including by the use of metadata, is an implementation of contextually or taxonomically associated data.

149. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such vaulting places aggregated select content into respective corresponding data stores. The Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. Compliant enterprises further "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. Such "Restoration Platform" understands "a standardized set of data for brokerage or deposit accounts." *See* Joint White Paper. As implemented, compliant systems establish corresponding storage units (or storage trees) in the vault. *See, e.g.,* PowerProtect User Guide at 52; *see also* Solution Guide at 25 (describing data trees). The aggregated select content can include data, such as binaries, boot images, and backup catalogs. *See, e.g.,* Solution Guide at 25.

150. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of (with respect to data processed by said cloud-based system) extracting and storing said security designated data in respective select content data stores.

151. The Accused Instrumentalities further comprise an apparatus which directly performs the step of activating at least one of said select content data stores in said cloud-based computing system 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. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault is safeguarded by a number of security measures, including strict credential-controlled access.

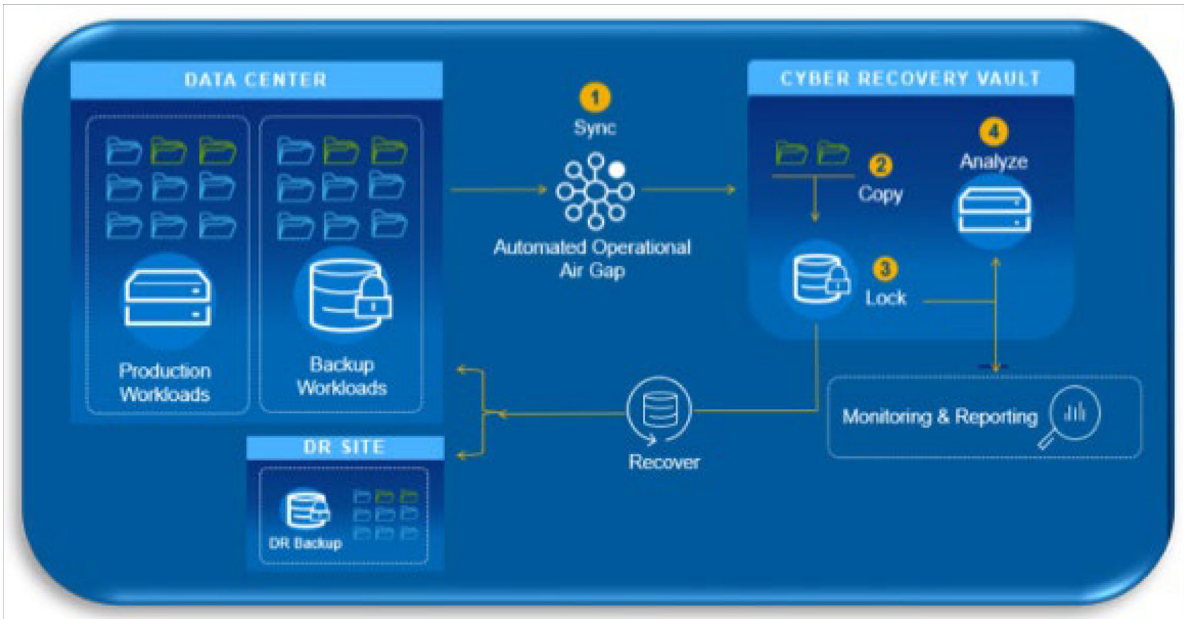
152. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which select content is protected "in a highly secure data vault." *See, e.g.,* Joint White Paper (further describing the data vault as "an ultra-secure environment where data can be safely stored, which remains inaccessible but secure even while being updated"). Such security measures are implemented via data vault access controls, which include multi-factor authentication. *See, e.g.,* Solution Guide at 21-22 (describing "least-access-privilege concept" and two-factor authentication); *see also* Dell PowerProtect Cyber Recovery 19.12 Product Guide, available at: dl.dell.com/content/manual52605381-dell-powerprotect-cyber-recovery-19-12-product-guide.pdf?language=en-us&ps=true (as visited October 20, 2023) (hereafter as "Dell Product Guide"), at 24 (describing process of defining storage objects for each system running in the vault environment).

153. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of activating at least one of said select content data stores in said cloud-based computing system 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.

154. The Accused Instrumentalities further comprise an apparatus which directly performs the step of parsing remainder data not extracted from data processed by said cloud-based system and storing the parsed data in respective granular data stores. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which non-extracted data is stored on the production side (*i.e.,* outside the data vault) in a plurality of data stores.

155. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Further, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider." *See* At-A-Glance. As implemented, remainder data is stored in a plurality of granular data stores, including production and backup systems. *See* Dell Digital Vault Solution at 7 (describing process of pulling data from backup storage on the production side); *see also* Dell PowerProtect Solution Brief (illustrating multiple granular data stores for non-extracted parsed data), as reproduced below:



see also Solution Guide at 26 ("In the production environment, *backups of applications and their data*, including image-level backups, are typically performed daily. Backups are made to one or more PowerProtect DD MTrees on the production PowerProtect DD system").

156. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of parsing remainder data not extracted from data processed by said cloud-based system and storing the parsed data in respective granular data stores.

157. The Accused Instrumentalities further comprise an apparatus which directly performs the step of (with respect to the aforementioned parsing and storing of remainder data) including both (i) randomly parsing and storing said remainder data, and (ii) parsing and storing said remainder data according to a predetermined algorithm based upon said security designated data and said select content data stores. More specifically, and on information and belief, and as

discussed herein above and below, the Accused Instrumentalities comprise a system in which data encryption methodologies are implemented across the production environment and the data vault.

158. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Further, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider." *See* At-A-Glance. As implemented, traffic to and from the data vault is encrypted (randomly parsed), as is data in the production environment.

159. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of parsing remainder data not extracted from data processed by said cloud-based system and storing the parsed data in respective granular data stores.

160. The Accused Instrumentalities further comprise an apparatus which directly performs the step of withdrawing some or all of said security designated data and said parsed data from said respective data stores only in the presence of said respective access controls applied thereto. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which strict access control measures are implemented to safeguard the data vault and allow for secure restoration.

161. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain

(extract) select content for protective vaulting. Further, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider." *See* At-A-Glance. Indeed, the very purpose of the Sheltered Harbor standard is to allow for the emergency restoration of critical select content in the aftermath of a "Sheltered Harbor Event" (*e.g.,* cyberattack). *See* At-A-Glance; *see also* Joint White Paper (Sheltered Harbor requires a "highly secure data vault" and planned recovery protocols; data vault must be "air-gapped" and strictly inaccessible to unauthorized bad actors; defining the "restoration platform"). As implemented, compliant systems create immutable copies of select content for secure storage in the data vault. Such data is able to be withdrawn from the data vault to the restoration platform only upon the satisfaction of strict security measures and access controls, including credentialed access and multi-factor authentication. *See, e.g.,* Joint White Paper (further describing the data vault as "an ultra-secure environment where data can be safely stored, which remains inaccessible but secure even while being updated"); *see also* Solution Guide at 21-22 (describing "least-access-privilege concept" and two-factor authentication); *see also id.* at 28-29 (describing cleansing and re-imaging data from the data vault to the production environment and restoration platform); *see also* Dell Product Guide at 24 (describing process of defining storage objects for each system running in the vault environment).

162. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of withdrawing some or all of said security designated data and said parsed data from said respective data stores only in the presence of said respective access controls applied thereto.

163. The foregoing infringement on the part of Defendant has caused past and ongoing injury to Plaintiff. The amount of damages adequate to compensate for the infringement shall be determined at trial but is in no event less than a reasonable royalty from the date of first infringement to the expiration of the '169 Patent.

164. To the extent Defendant continues, and has continued, its infringing activities noted above in an infringing manner post-notice of the '169 Patent, such infringement is necessarily willful and deliberate.

165. Each of Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

COUNT III
Infringement of U.S. Patent No. 10,182.073

166. Plaintiff incorporates the above paragraphs by reference.

167. Upon information and belief, Defendant owns and/or controls the operation and/or utilization of the Accused Instrumentalities and generates substantial financial revenues therefrom, including but not limited to revenues attributable to business reputation and goodwill, and revenues derived from consumer confidence in the Defendant's ability to protect against cyber threats and maintain operations regardless of external attack or internal system failure.

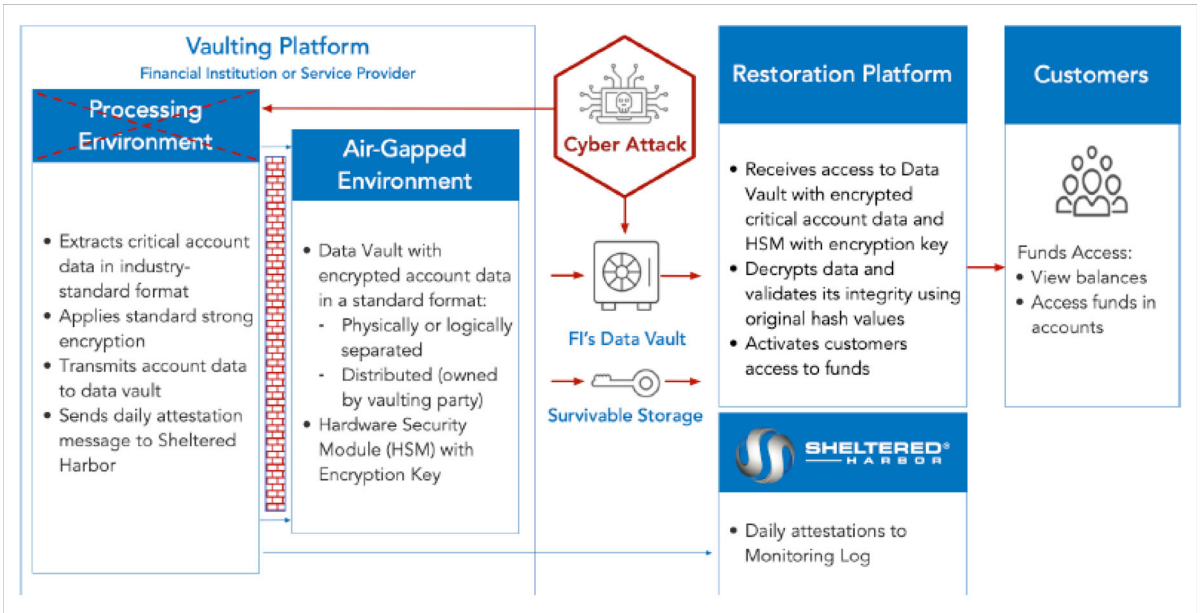
168. Upon information and belief, Defendant has directly infringed and continues to directly infringe at least Claim 1 of the '073 Patent by making, using, importing, selling, and/or offering for sale the Accused Instrumentalities. The Accused Instrumentalities themselves are specially configured by Defendant to directly perform, and do in fact directly perform, all infringing steps.

169. Upon information and belief, the Accused Instrumentalities comprise an

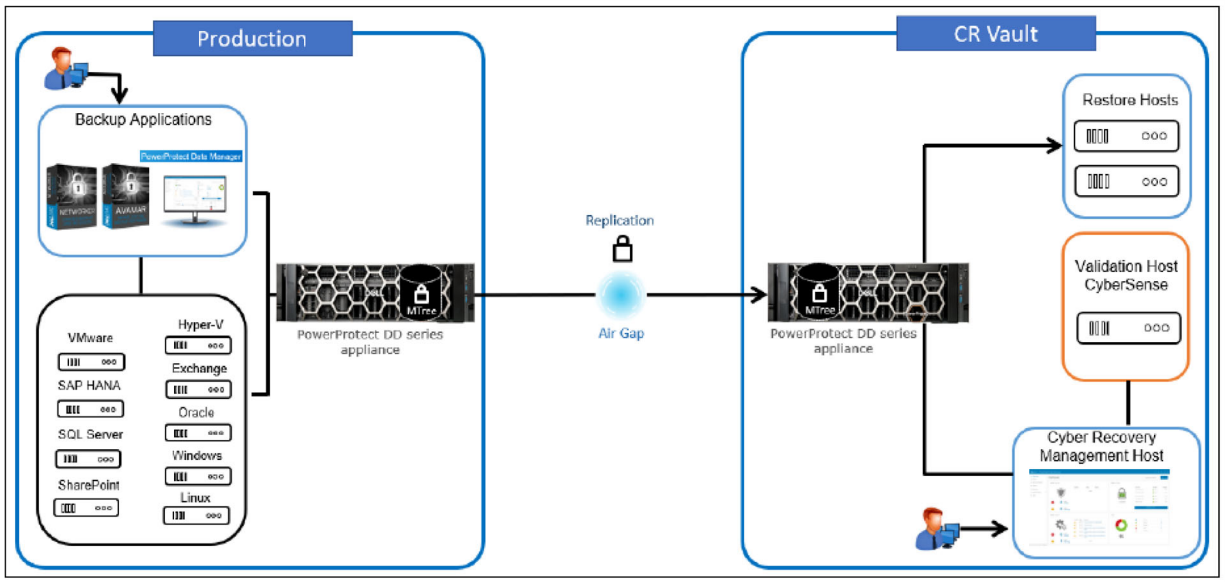
apparatus which directly performs the claimed method of creating an information infrastructure for processing data throughput in a distributed computing system with respective ones of a plurality of filters. More specifically, the Accused Instrumentalities comprise a network of servers, hardware, and software for processing data and vaulting such data in compliance with Sheltered Harbor specifications or its operational equivalent, as described herein above. The Defendant is the "enterprise operating the distributed computing system," and Defendant itself makes and uses the system, owns all data, and controls the data vault. *See, e.g.,* Joint White Paper (Sheltered Harbor standard requires: "Data fully Owned, and vault Controlled by the financial institution"); *see also* Cobalt Iron White Paper ("The data vault always remains under your control").

170. On information and belief, such apparatus is installed and used in the United States, and such apparatus performs the infringing steps entirely within the United States.

171. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content in distributed computing systems. See, e.g., Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):



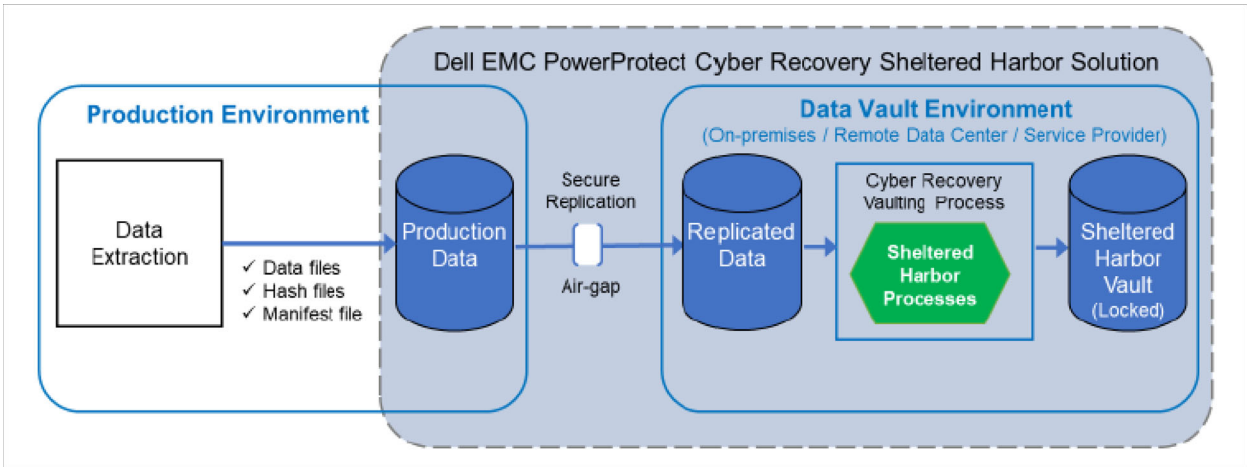
see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:



172. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Operating Rules at Exhibit 1 thereof (stating the Processing Environment "Extracts *critical account data* in industry-standard format"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect any data that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an entire backup application and its backup data, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees").

174. As implemented in compliant systems, the Sheltered Harbor standard is satisfied by an information infrastructure for processing data throughput in the form of critical account information from the enterprise to the data vault. *See, e.g.,* Dell Sheltered Harbor Solution Brief ("To comply with the Sheltered Harbor Specification, the Cyber Recovery vault architecture has been extended to perform the Archive Generation and Secure Repository processes. Extracted Sheltered Harbor data is saved in production, then securely replicated via a logical, air-gapped, dedicated connection to the vaulted environment where the remaining steps, such as retention locking, are performed"); *see also id.,* illustrating the compliant information infrastructure as

excerpted below:



175. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the claimed method of creating an information infrastructure for processing data throughput in a distributed computing system with respective ones of a plurality of filters.

176. The Accused Instrumentalities further comprise an apparatus which directly performs the step of identifying sensitive content and select content in said data throughput with respective initially configured filters of said plurality of filters, said sensitive content represented by one or more sensitive words, characters, images, data elements or data objects therein grouped into a plurality of sensitivity levels, said select content represented by one or more predetermined words, characters, images, data elements or data objects. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a data vault with designated stores for designated select content, as derived from categorical filters.

177. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is represented by predetermined words, characters, images, data elements, or objects. *See, e.g.,* Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect *any data* that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an *entire backup application and its backup data*, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees") (and further identifying " *Data, such as application binaries, boot images, and backup catalog*, that must be protected").

178. Still further, the Sheltered Harbor standard is satisfied by systems in which a plurality of initially configured filters are used to identify the select content for filtering, extraction, and secure vault storage. Such systems use dynamic filters as configured by the operating enterprise in order to define the select content and the treatment thereof. As noted, the Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Such data vault is intended to house content derived from designated categorical filters, as established by the enterprise. As explained, the fundamental first step in the Sheltered Harbor process is to: " *Identify the most critical business services that must be protected* and resilient in the face of an 'extreme but plausible event,' and

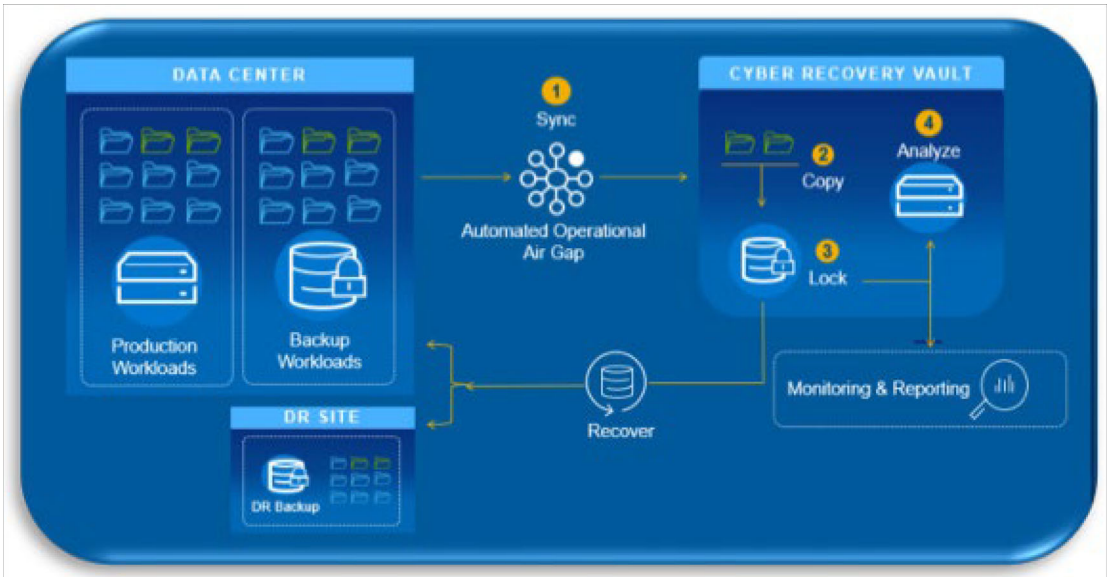
ultimately *map these to the IT data and/or applications necessary to support them*." *See* Joint White Paper. Further, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform ... for those two critical business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format"). As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52.

179. In view of the foregoing, and on information and belief, the Accused

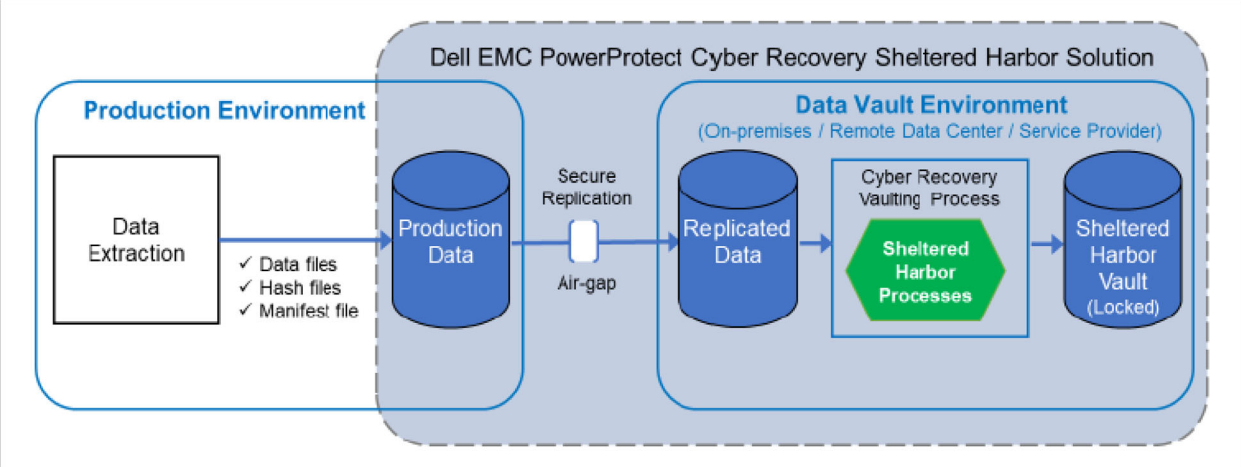
Instrumentalities thus comprise an apparatus which directly performs the claimed step of identifying sensitive content and select content in said data throughput with respective initially configured filters of said plurality of filters, said sensitive content represented by one or more sensitive words, characters, images, data elements or data objects therein grouped into a plurality of sensitivity levels, said select content represented by one or more predetermined words, characters, images, data elements or data objects.

180. The Accused Instrumentalities further comprise an apparatus which directly performs the step of providing in said distributed computing system a plurality of secure sensitive content data stores and a plurality of select content data stores for said respective initial filters. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a data vault with designated stores for designated select content, as derived from categorical filters.

181. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is stored in a plurality of select content data stores. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. By way of example, and as implemented in compliant systems, the authorized solution from Dell includes a plurality of such data stores, as illustrated below (*see* Dell PowerProtect Solution Brief) (illustrating multiple data stores, including Backup, Copy, Lock, and Analyze):



see also PowerProtect User Guide at 52 (stating "When you create a protection policy, the PowerProtect Data Manager software *creates a storage unit on the specified Data Domain backup host* that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*"); *see also* Dell Sheltered Harbor Solution Brief (illustrating the compliant information infrastructure, which includes a plurality of secure sensitive content data stores, as excerpted below:)



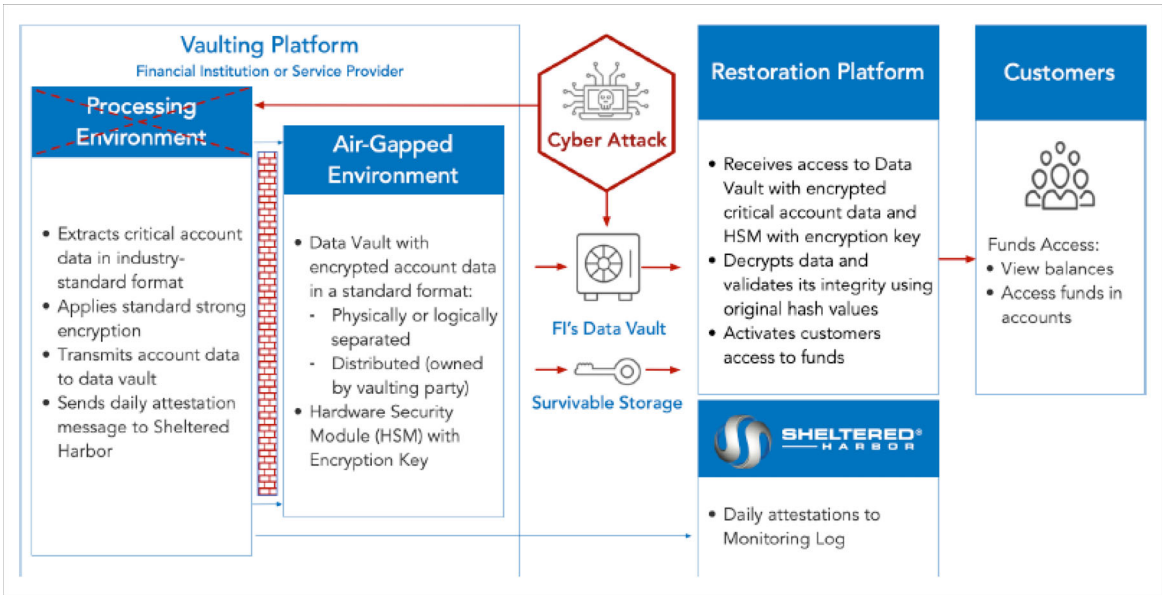
182. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the data stores for the sensitive content are operative with a plurality of designated categorical filters. As noted, the Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. Such data vault is intended to house content derived from designated categorical filters, as established by the enterprise. As explained, the fundamental first step in the Sheltered Harbor process is to: " *Identify the most critical business services that must be protected* and resilient in the face of an 'extreme but plausible event,' and ultimately *map these to the IT data and/or applications necessary to support them*." *See* Joint White Paper. Further, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and

underlying technologies, enabling the creation of a common restoration platform ... for those two critical business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format"). As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52.

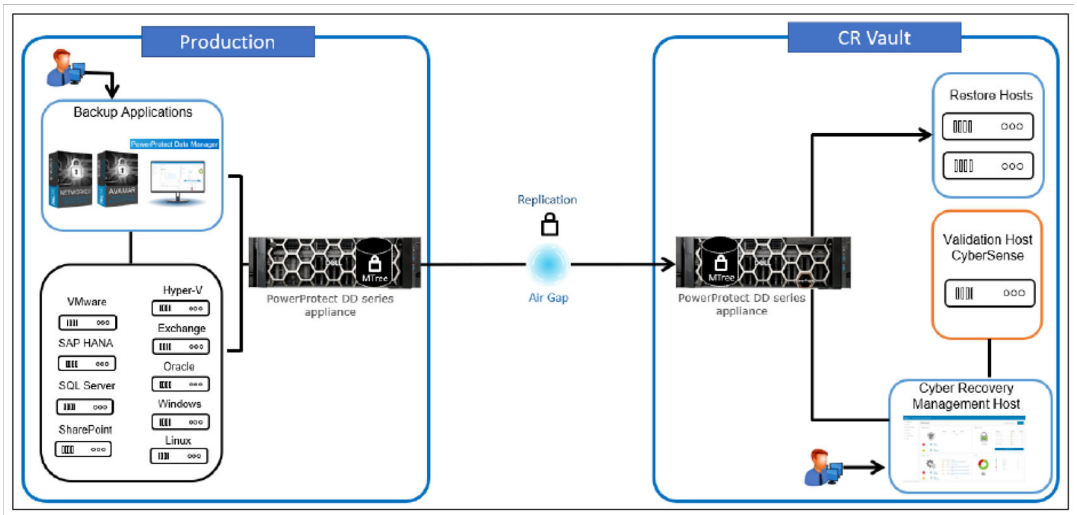
183. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of providing in said distributed computing system a plurality of secure sensitive content data stores and a plurality of select content data stores for said respective initial filters.

184. The Accused Instrumentalities further comprise an apparatus which directly performs the step of operatively coupling said respective initially configured filters, over a communications network with said distributed computing system, said plurality of sensitive content data stores and said select content data stores. More specifically, and on information and

belief, and as discussed herein above and below, the Accused Instrumentalities comprise a distributed computing system which is configured to manage and protect data containing sensitive content. *See, e.g.,* Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below (illustrating distributed network architecture):

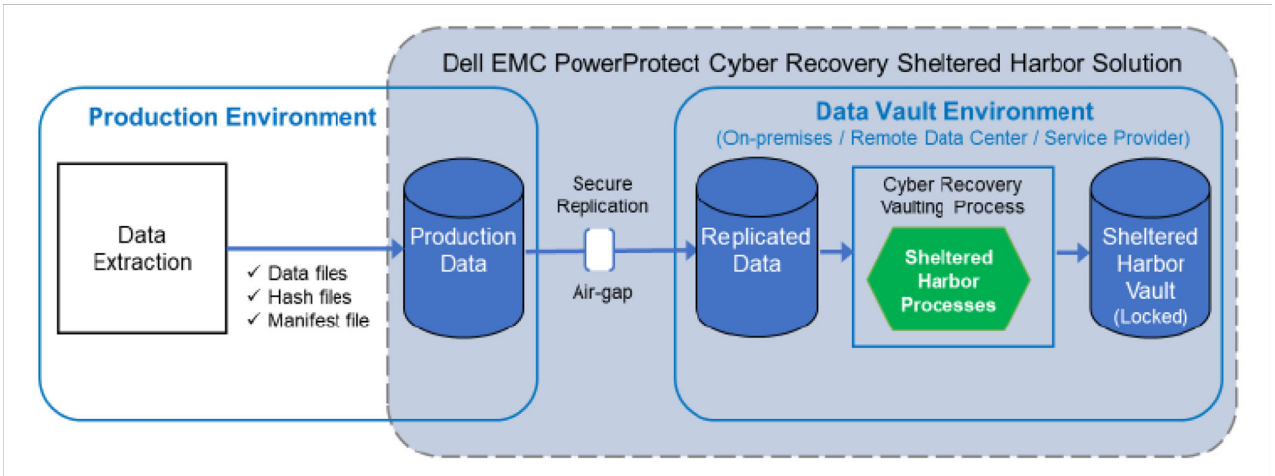


see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed



architecture), as reproduced below:

185. Such systems as implemented by Defendant necessarily comprise an operatively coupled communications network which couples the production and vaulting environments. See, e.g., Dell Digital Vault Solution at 7 (describing network with dedicated interfaces); see also At-A-Glance (data vault is required to be "completely separated" from the infrastructure of the compliant Case 2:23-cv-00550 Document 1 Filed 11/21/23 Page 92 of 116 PageID #: 92 ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT 93 enterprise; also describing the "restoration platform"); see also Joint White Paper (Sheltered Harbor requires data vault to be both "survivable" and "accessible"); see also Dell Sheltered Harbor Solution Brief (illustrating the compliant information infrastructure, which includes a communication network operatively coupling the production and data vault environments (via a "logical, air-gapped, dedicated connection"), as excerpted below:)



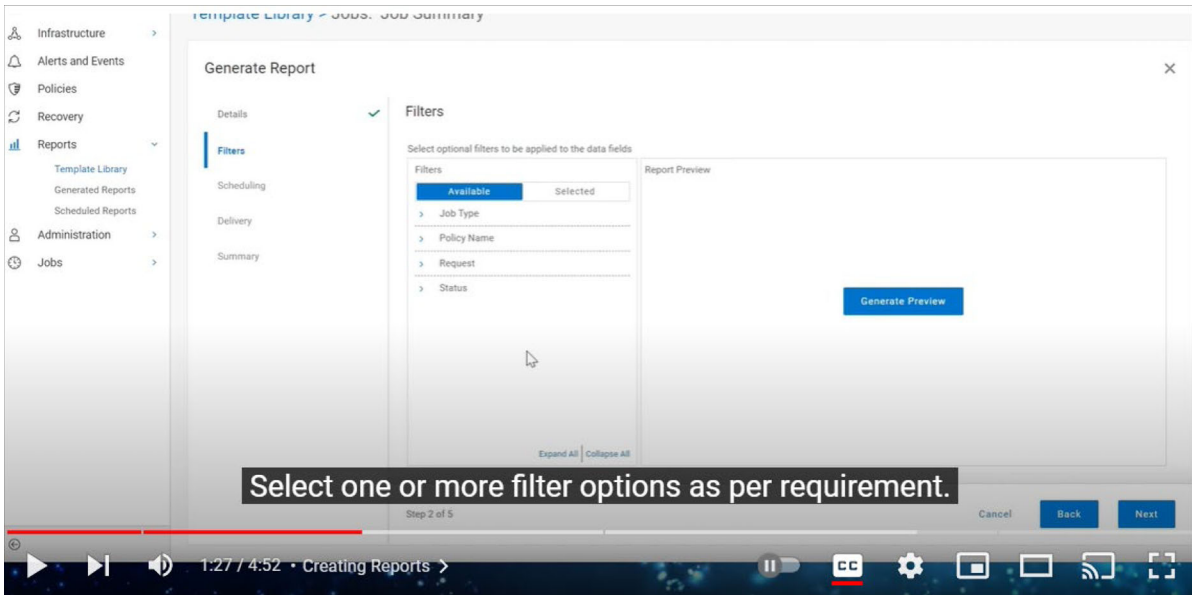
186. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of operatively

coupling said respective initially configured filters, over a communications network with said distributed computing system, said plurality of sensitive content data stores and said select content data stores.

187. The Accused Instrumentalities further comprise an apparatus which directly performs the step of altering said respective initially configured filters by: expanding one or both of said sensitive content and said select content in a designated filter, contracting or reducing one or both of said sensitive content and said select content in said designated filter, and imposing or removing a hierarchical or an orthogonal classification in said designated filter. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which protection policies are implemented using aggregated tags, and such tags (and their respective policies) are enabled for modification (expansion and contraction) by the operating enterprise.

188. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industrystandard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, this includes the process of defining policies relating to the identification and extraction of select content, and the ongoing evaluation and modification of such policies, by the compliant operating enterprise. By way of example, in the certified Dell PowerProtect system, "the Cyber Recovery User Interface [UI] is the primary tool for performing and monitoring Cyber Recovery operations. It is a web application that *enables you to define, run, and monitor*

policies and policy outcomes." *See* Dell Product Guide at 20. Further, the compliant system allows the operating enterprise to: " *Create policies* to perform replications, make point-in-time (PIT) copies, set retention locks, and perform other Cyber Recovery operations within the Cyber Recovery vault. You can also *modify existing policies*."). *See* Dell Product Guide at 30. Policy modification provides for the expansion and reduction of existing parameters. *See, e.g.,* Dell Instructional Video entitled: Reporting with PowerProtect Cyber Recovery, available at: youtube.com/watch?v=KTW5htQxyn0&t=85s (as visited October 20, 2023) (hereafter as "Dell Instructional Video"), at 1:24-1:50, as excerpted below:



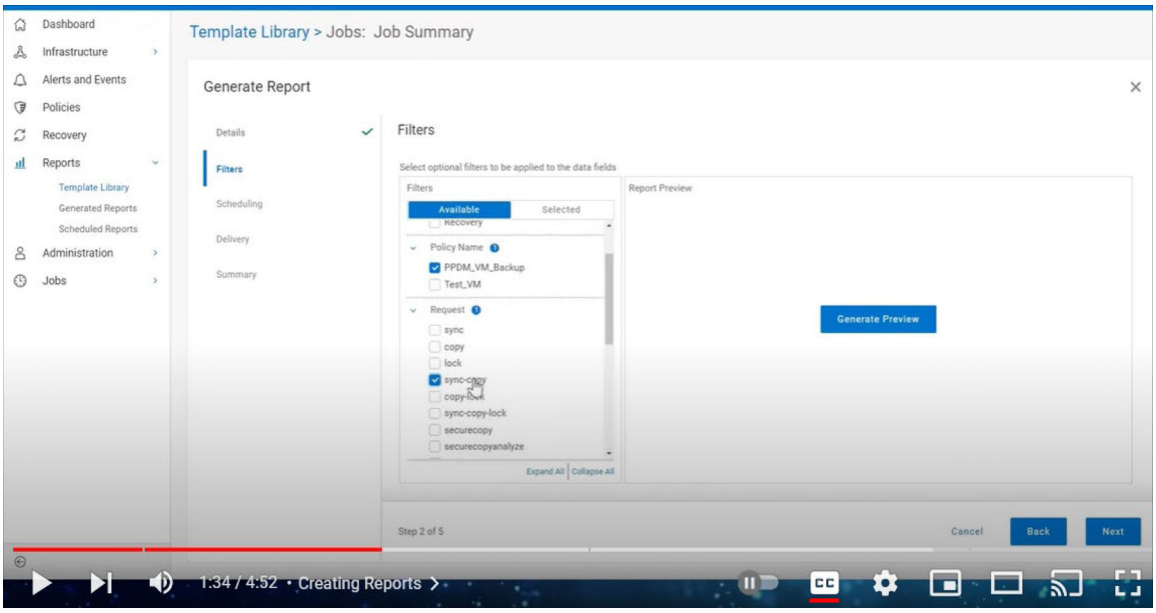
189. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of altering said respective initially configured filters by: expanding one or both of said sensitive content and said

select content in a designated filter, contracting or reducing one or both of said sensitive content and said select content in said designated filter, and imposing or removing a hierarchical or an orthogonal classification in said designated filter.

190. The Accused Instrumentalities further comprise an apparatus which directly performs the steps of generating modified configured filters based upon said alterations with said designated filter; and organizing further data throughput in said distributed computing system with said modified configured filters. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise in which protection policies are implemented using aggregated tags, and such tags (and their respective policies) are enabled for modification (expansion and contraction) by the operating enterprise. Such modification is dynamic and the resulting parameters are thereafter implemented by the system.

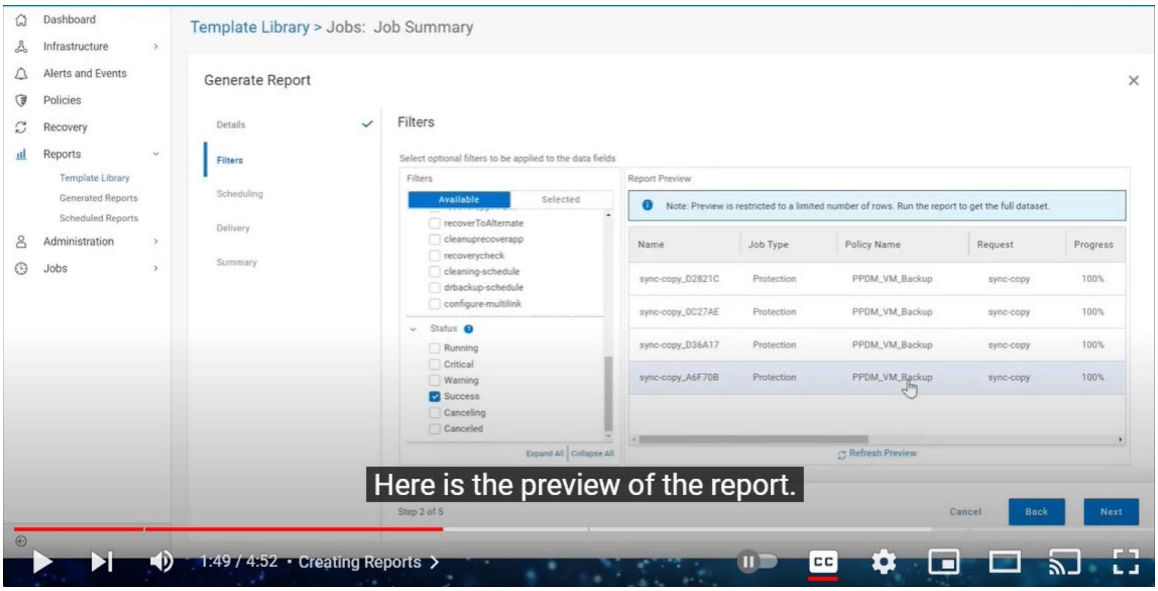
191. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industrystandard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. Again as noted above, as implemented, this includes the process of defining policies relating to the identification and extraction of select content, and the ongoing evaluation and modification of such policies, by the compliant operating enterprise. By way of example, in the certified Dell PowerProtect system, "the Cyber Recovery User Interface [UI] is the primary tool for performing and monitoring Cyber Recovery operations. It is a web application that *enables you to define, run, and monitor policies and policy outcomes*." *See* Dell Product Guide at 20. Further,

the compliant system allows the operating enterprise to: " *Create policies* to perform replications, make point-in-time (PIT) copies, set retention locks, and perform other Cyber Recovery operations within the Cyber Recovery vault. You can also *modify existing policies*."). *See* Dell Product Guide at 30. Policy modification provides for the expansion and reduction of existing parameters, which dynamically generates modified configured filters and organizes further data throughput in accordance with the new configuration. *See, e.g.,* Dell Instructional Video at 1:24-1:50, as excerpted below:



192. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the steps of generating modified configured filters based upon said alterations with said designated filter; and organizing further data throughput in said distributed computing system with said modified configured filters.

193. The foregoing infringement on the part of Defendant has caused past and ongoing injury to Plaintiff. The amount of damages adequate to compensate for the infringement shall be determined at trial but is in no event less than a reasonable royalty from the date of first infringement to the expiration of the '073 Patent.



194. To the extent Defendant continues, and has continued, its infringing activities noted above in an infringing manner post-notice of the '073 Patent, such infringement is necessarily willful and deliberate.

195. Each of Defendant's aforesaid activities have been without authority and/or

license from Plaintiff.

COUNT IV
Infringement of U.S. Patent No. 10,250,639

196. Plaintiff incorporates the above paragraphs by reference.

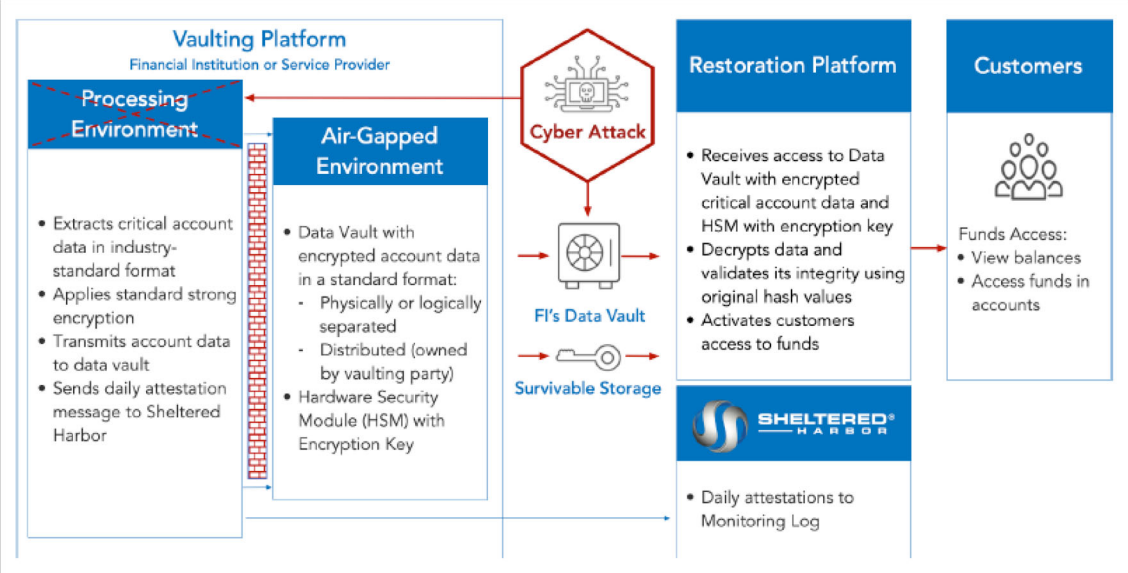
197. Upon information and belief, Defendant owns and/or controls the operation and/or utilization of the Accused Instrumentalities and generates substantial financial revenues therefrom, including but not limited to revenues attributable to business reputation and goodwill, and revenues derived from consumer confidence in the Defendant's ability to protect against cyber threats and maintain operations regardless of external attack or internal system failure.

198. Upon information and belief, Defendant has directly infringed and continues to directly infringe at least Claim 16 of the '639 Patent by making, using, importing, selling, and/or offering for sale the Accused Instrumentalities. The Accused Instrumentalities themselves are specially configured by Defendant to directly perform, and do in fact directly perform, all infringing steps.

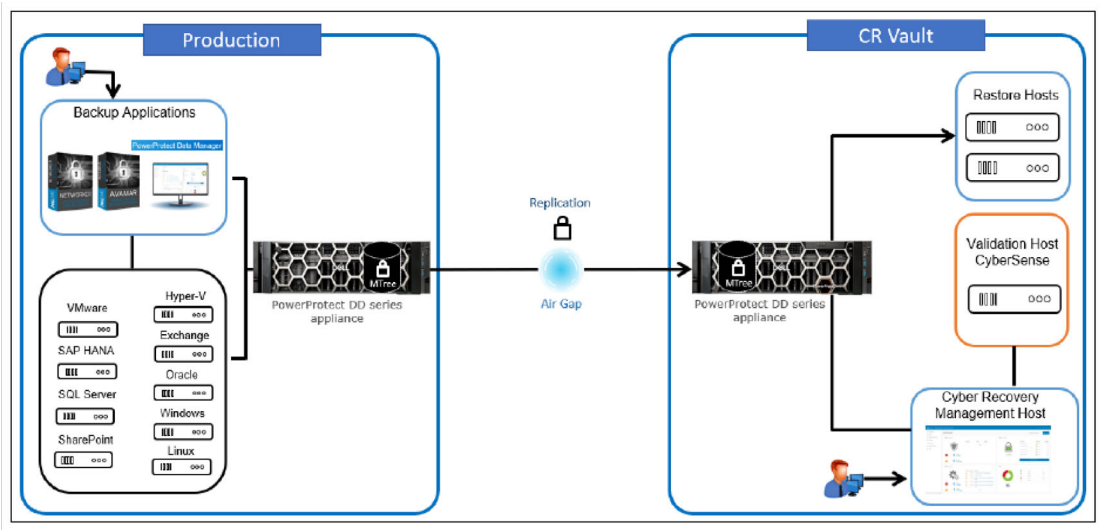
199. Upon information and belief, the Accused Instrumentalities comprise an apparatus which directly performs the claimed method of sanitizing data processed in a distributed computing system having sensitive content and select content, said sensitive content represented by one or more sensitive words, characters, images, data elements or data objects therein, said sensitive content having a plurality of sensitivity levels, each sensitivity level having an associated security clearance, said select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of extract data stores for respective ones of said plurality of sensitivity levels and having a plurality of select content data stores, said plurality of extract data

stores and said select content data stores operatively coupled over a communications network. More specifically, the Accused Instrumentalities comprise a network of servers, hardware, and software for processing data and vaulting such data in compliance with Sheltered Harbor specifications or its operational equivalent, as described herein above. The Defendant is the "enterprise operating the distributed computing system," and Defendant itself makes and uses the system, owns all data, and controls the data vault. *See, e.g.,* Joint White Paper (Sheltered Harbor standard requires: "Data fully Owned, and vault Controlled by the financial institution"); *see also* Cobalt Iron White Paper ("The data vault always remains under your control"). On information and belief, such apparatus is installed and used in the United States, and such apparatus performs the infringing steps entirely within the United States.

200. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content in distributed computing systems. *See, e.g.,* Operating Rules (the Sheltered Harbor objective of protecting critical account information is achieved by data vaulting); *see also id,* at Exhibit 1 thereof, as reproduced below



(illustrating distributed network architecture):



see also Reference Architecture (illustrating Sheltered Harbor compliant system and distributed architecture), as reproduced below:

201. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. See, e.g., Operating Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting critical account information and data sets of market participants in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability").

202. Still further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the sensitive content to be protected is represented by one or more sensitive words, characters, images, data elements or data objects therein. *See, e.g.,* Operating

Rules ("Sheltered Harbor is an industry-driven initiative launched in 2015 to promote the stability of the U.S. financial markets by protecting *critical account information and data sets of market participants* in order to facilitate the recovery and use of such information following a destructive cyberattack or other extreme loss of operational capability"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect *any data* that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an *entire backup application and its backup data*, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees") (and further identifying " *Data, such as application binaries, boot images, and backup catalog*, that must be protected").

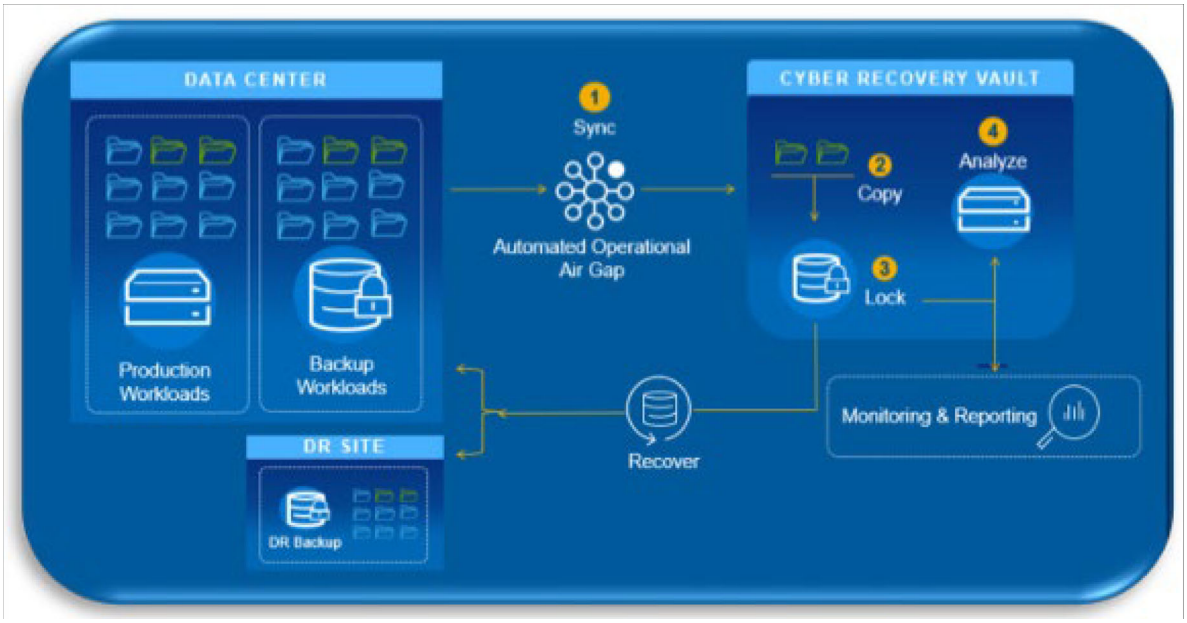
203. Still further, the sensitive content to be protected is associated with multiple security levels and clearance requirements, as established by the Sheltered Harbor compliant enterprise. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which select content is protected "in a highly secure data vault." *See, e.g.,* Joint White Paper (further describing the data vault as "an ultra-secure environment where data can be safely stored, which remains inaccessible but secure even while being updated"). As implemented, sensitive content is protected via priority filters. *See, e.g.,* PowerProtect User Guide at 146 ("When multiple dynamic filters exist, *you can define the priority of the dynamic filter*. Priority determines which dynamic filter PowerProtect Data Manager applies for an asset if an asset matches multiple dynamic filters, and if the matching dynamic filters have conflicting actions. For example, if an asset protection policy assignment matches *several dynamic filters and each*

dynamic filter specifies a different protection policy assignment, the protection policy is determined by the dynamic filter with the highest priority. An integer is used to represent the priority of the dynamic filter. The smaller value has the *higher priority*"). Again, and as noted above, Sheltered Harbor emphasizes secure vaulting and reconstruction, and vaulted data is accessible only via strict credential control. *See, e.g.,* Dell PowerProtect Solution Brief (explaining: "An isolated data center environment that is disconnected from corporate and backup networks and *restricted from users other than those with proper clearance*").

204. Still further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems which manage and protect data containing sensitive content which is important to the operating enterprise; namely, customer financial account data. *See, e.g.,* Operating Rules. Critical account data is extracted and converted into Sheltered Harbor's standard format, and select content is represented by one or more predetermined words, characters, images, data elements or data objects. *See* Operating Rules at Exhibit 1 thereof (stating the Processing Environment "Extracts *critical account data* in industry-standard format"); *see also* Solution Guide at 25 ("In addition to determining the objectives for the Cyber Recovery solution, you must *characterize the data to be protected*. The Cyber Recovery solution can protect any data that can be stored on a PowerProtect DD MTree. If Cyber Recovery is to protect an entire backup application and its backup data, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more PowerProtect DD MTrees"); *see also* Solution Guide at 25 (The aggregated select content can include data, such as binaries, boot images, and backup catalogs).

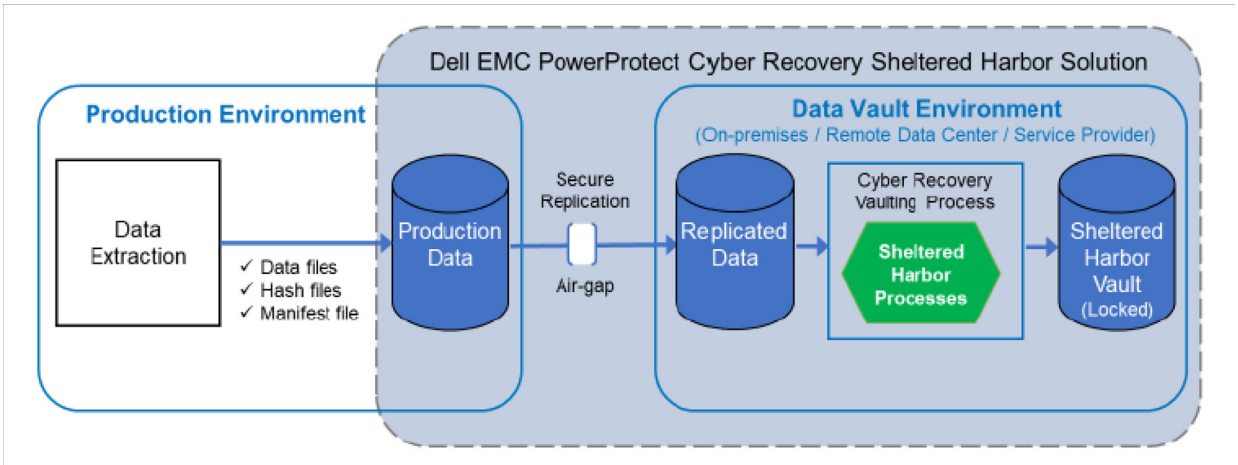
205. Still further, and as noted above, the Sheltered Harbor standard requires, and is

satisfied by, systems in which the sensitive select content to be protected is stored in a plurality of select content data stores. The Sheltered Harbor standard requires a "data vault," which is an "ultra secure environment where data can be safely stored." *See* Joint White Paper. By way of example, and as implemented in compliant systems, the authorized solution from Dell includes a plurality of such data stores, as illustrated below (*see* Dell PowerProtect Solution Brief) (illustrating multiple data stores, including Backup, Copy, Lock, and Analyze):



see also PowerProtect User Guide at 52 (stating "When you create a protection policy, the PowerProtect Data Manager software *creates a storage unit on the specified Data Domain backup host* that is managed by PowerProtect Data Manager. *All subsequent backups will go to this new storage unit*") *see also* Dell Sheltered Harbor Solution Brief (illustrating the compliant information infrastructure, which includes a communication network operatively coupling the production and data vault environments (via a "logical, air-gapped, dedicated connection"), as

excerpted below:)



206. Yet still further, and as noted above, Sheltered Harbor requires the compliant enterprise to: "Protect *the data and/or applications supporting the processes* in a highly secure data vault, defining the requirements necessary for such a vault." *See* Joint White Paper. Given the focus of Sheltered Harbor, the primary designated categorical filters relate to "two capabilities and essential services: *providing customers continued access to their account balance information and cash*. [...] By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform ... for those two critical business services." *See* Joint White Paper. As a result, "[t]he Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario." *See* Joint White Paper. As a collective, Sheltered Harbor has thus "done the work of *defining the critical business processes* as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions." *See* Joint White Paper. This is

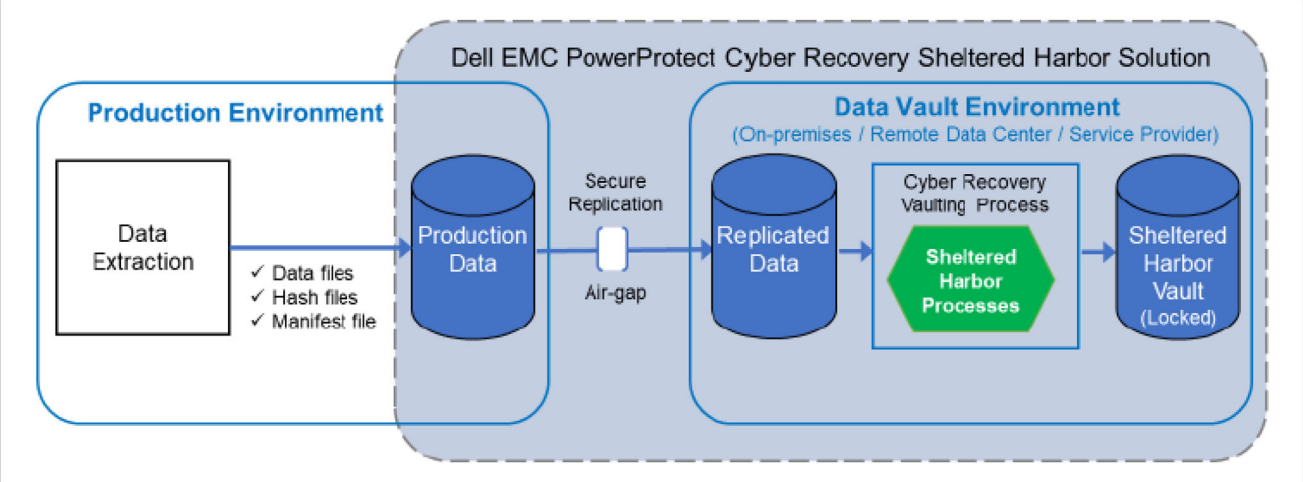
accomplished by the extraction of critical account data, which is identified based upon predefined filters. *See* Operating Rules at Exhibit 1 thereof (Processing Environment: " *Extracts critical account data* in industry-standard format"); *see also* Safe Haven (explaining: " When a financial institution joins Sheltered Harbor, *critical financial information is extracted* from accounts and converted into Sheltered Harbor's industry-standard format"). As implemented, the enterprise establishes a "protection policy" (*i.e.,* a set of filters) governing the data to be protected. *See* PowerProtect User Guide at 52. Of course, each data store includes access controls, as implemented via sensitivity levels using security credentials and/or multi-factor authentication, or a functional equivalent. *See, e.g.,* Solution Guide at 21-22 (describing data access protocols).

207. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the claimed method of sanitizing data processed in a distributed computing system having sensitive content and select content, said sensitive content represented by one or more sensitive words, characters, images, data elements or data objects therein, said sensitive content having a plurality of sensitivity levels, each sensitivity level having an associated security clearance, said select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of extract data stores for respective ones of said plurality of sensitivity levels and having a plurality of select content data stores, said plurality of extract data stores and said select content data stores operatively coupled over a communications network.

208. The Accused Instrumentalities comprise an apparatus which directly performs the

step of extracting said sensitive content from a data input to obtain extracted sensitive data for a corresponding sensitivity level and remainder data. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which protection policies are implemented using aggregated tags.

209. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industrystandard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof; *see also* Dell Sheltered Harbor Solution Brief (illustrating the compliant information infrastructure, which includes data extraction in the production environment and secure storage in the data vault, as excerpted below:)



210. Yet still further, and as implemented, this process includes the selection of protection policies by the enterprise, and the selection of conditions for each such policy. *See*

Virtual Machine User Guide at 57. Protection rules are one exemplary embodiment of such categorical filters, which can be implemented in a variety of functionally equivalent ways to achieve the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, "a rule with the filters VM Folder Name, Contains, and Finance can match assets belonging to your finance department to the selected protection policy." *See* Virtual Machine User Guide at 58. The use of such protection rules and attributes for filtering content is a type of categorical filter implementation. *See* Virtual Machine User Guide at 58-59 (detailing use of Protection Rule Attributes, Conditions, Criteria, and Filters (*e.g.,* "contains," "does not contain," "does not equal," "ends with," "equals," "matches RegEx," and "does not match RegEx")).

211. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which critical financial account information is extracted and converted into Sheltered Harbor's industry-standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, the extracted information is either contextually or taxonomically associated. As explained by the inventors: "A simple classification system (hierarchical taxonomic system) can be established by reviewing the label descriptions on the structured data and then expanding class definitions with the use of the Knowledge Expander (KE) search engine. [...] The hierarchical taxonomic system can be used to build contextual filters and taxonomic filters which can further protect Sec-Con data and expand the value and quantity of SC data." *See* '301 Patent at 10:22-32. In practice, Sheltered Harbor systems allow for the grouping of tags using metadata or any of a number of functionally equivalent means of achieving the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell

PowerProtect system, virtual machine tags are created in the "vSphere Client." Such virtual tags enable the enterprise to attach metadata to virtual inventory assets, making them easier to sort and search. *See* Virtual Machine User Guide at 56. Tags are grouped within categories, which can further include specific object types. *See* Virtual Machine User Guide at 56-58 (describing tag creation and protection rules). The use of tag grouping, including by the use of metadata, is an implementation of contextually or taxonomically associated data.

212. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such vaulting places aggregated select content into respective corresponding data stores. The Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. Compliant enterprises further "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. Such "Restoration Platform" understands "a standardized set of data for brokerage or deposit accounts." *See* Joint White Paper. As implemented, compliant systems establish corresponding storage units (or storage trees) in the vault. *See, e.g.,* PowerProtect User Guide at 52; *see also* Solution Guide at 25 (describing data trees). The aggregated select content can include data, such as binaries, boot images, and backup catalogs. *See, e.g.,* Solution Guide at 25.

213. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of extracting said sensitive content from a data input to obtain extracted sensitive data for a corresponding sensitivity level and remainder data.

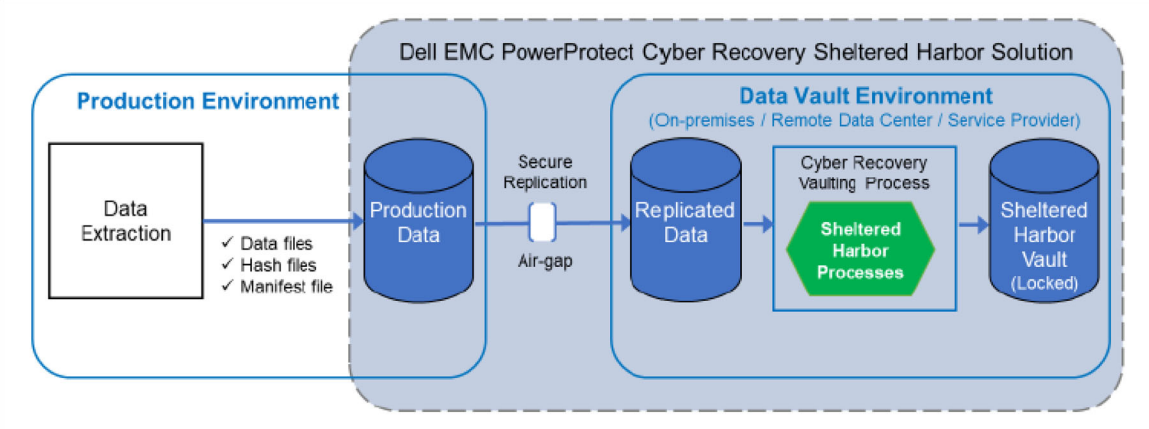
214. The Accused Instrumentalities further comprise an apparatus which directly performs the step of storing said extracted sensitive data for said corresponding sensitivity level in a respective secure extract store in said distributed computer system. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which the data storage vault stores select content for a designated set of account data, which includes binaries and backups.

215. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Such vaulting places aggregated select content into corresponding data stores. The Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider. The data vault [*e.g.,* corresponding data store] is encrypted, unchangeable, and completely separated from the institution's infrastructure, including all backups." *See* At-A-Glance. Compliant enterprises further "designate a restoration platform so that if the Sheltered Harbor Resiliency Plan is activated, the platform can recover data from the vault to restore customer funds access as quickly as possible." *See* At-A-Glance. Such "Restoration Platform" understands "a standardized set of data for brokerage or deposit accounts." *See* Joint White Paper. As implemented,

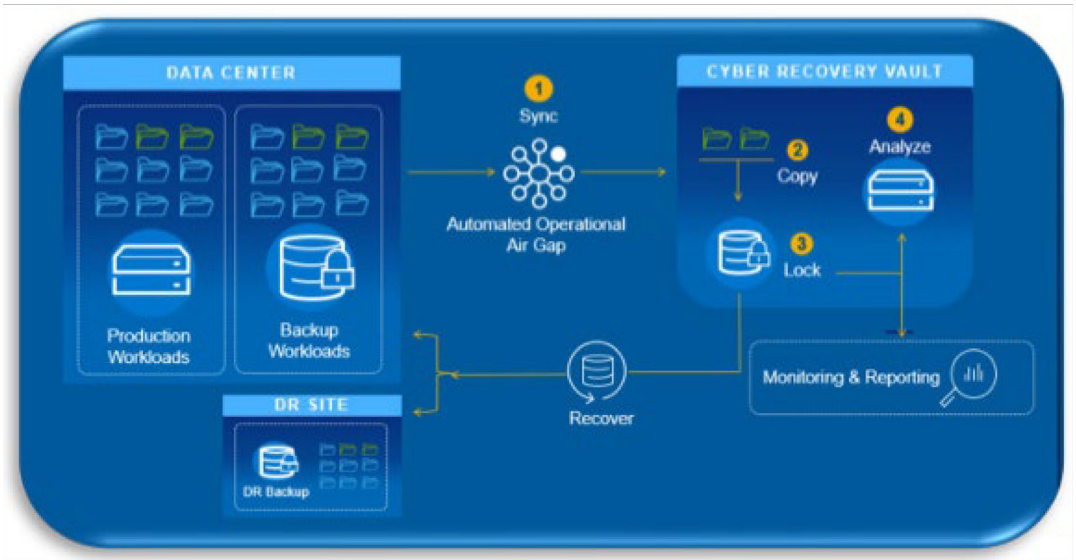
compliant systems establish corresponding storage units (or storage trees) in the vault. *See, e.g.,* PowerProtect User Guide at 52; *see also* Solution Guide at 25 (describing data trees). The aggregated select content can include data, such as binaries, boot images, and backup catalogs. *See, e.g.,* Solution Guide at 25.

216. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of storing said extracted sensitive data for said corresponding sensitivity level in a respective secure extract store in said distributed computer system.

217. The Accused Instrumentalities further comprise an apparatus which directly performs the step of extracting said select content from either said data input or said remainder data and storing extracted select content in said select content data stores. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which extracted select data is stored in the secure data vault, while non-extracted data is stored on the production side (*i.e.,* outside the data vault) in a plurality of data stores. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. *See, e.g.,* Dell Sheltered Harbor Solution Brief (illustrating the compliant information infrastructure, which includes data extraction in the production environment and secure storage in the data vault, as excerpted below:)



218. Further, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider." *See* At-A-Glance. As implemented, remainder data is stored in a plurality of granular data stores, including production and backup systems. *See* Dell Digital Vault Solution at 7 (describing process of pulling data from backup storage on the production side); *see also* Dell PowerProtect Solution Brief (illustrating multiple



granular data stores for non-extracted parsed data), as reproduced below:

see also Solution Guide at 26 ("In the production environment, *backups of applications and their data*, including image-level backups, are typically performed daily. Backups are made to one or more PowerProtect DD MTrees on the production PowerProtect DD system").

219. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of extracting said select content from either said data input or said remainder data and storing extracted select content in said select content data stores.

220. The Accused Instrumentalities further comprise an apparatus which directly results in the creation of sanitized sensitive content data and select content data from the non-extracted data from said select content extraction and remainder data from said sensitive content extraction. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which sensitive account data is extracted for secure storage in a data vault, thereby creating sanitized storage versions of the data.

221. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. Further, the Sheltered Harbor standard requires compliant enterprises to "back up critical customer account data each night in the Sheltered Harbor standard format, either managing their own vault or using their service provider." *See* At-A-Glance. This process results in the creation of sanitized sensitive content data and select content data from the non-extracted data from said select content extraction and remainder data

from said sensitive content extraction. Indeed, the express purpose of the Sheltered Harbor standard is to "protect public confidence in the U.S. financial system if a devastating event like a cyberattack causes an institution's critical systems – including backups – to fail." *See* At-A-Glance (further stating that Sheltered Harbor was created "to promote the stability of U.S. financial markets by protecting critical account information of market participants in order to facilitate recovery of such information").

222. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of parsing remainder data not extracted from data processed by said cloud-based system and storing the parsed data in respective granular data stores.

223. The Accused Instrumentalities further comprise an apparatus which directly performs the step of inferencing said sanitized sensitive content data and select content data with (a) a content filter, (b) a contextual filter, and (c) a taxonomic filter; and obtaining an inferenced sensitive content data and an inferenced select content data therefrom. More specifically, and on information and belief, and as discussed herein above and below, the Accused Instrumentalities comprise a system in which filters are utilized for the inferencing of content.

224. As noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which the plurality of designated categorical filters are activated in order to obtain (extract) select content for protective vaulting. As noted, the Sheltered Harbor standard is premised on the extraction of critical financial account information, which is then converted into Sheltered Harbor's industrystandard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, this includes the selection of protection policies by the enterprise, and the selection

of conditions for each such policy. *See* Virtual Machine User Guide at 57. Protection rules are one exemplary embodiment of such categorical filters, which can be implemented in a variety of functionally equivalent ways to achieve the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell PowerProtect system, "a rule with the filters VM Folder Name, Contains, and Finance can match assets belonging to your finance department to the selected protection policy." *See* Virtual Machine User Guide at 58. The use of such protection rules and attributes for filtering content is a type of categorical filter implementation. *See* Virtual Machine User Guide at 58-59 (detailing use of Protection Rule Attributes, Conditions, Criteria, and Filters (*e.g.,* "contains," "does not contain," "does not equal," "ends with," "equals," "matches RegEx," and "does not match RegEx")).

225. Further, and as noted above, the Sheltered Harbor standard requires, and is satisfied by, systems in which critical financial account information is extracted and converted into Sheltered Harbor's industry-standard format. *See, e.g.,* Operating Rules at Exhibit 1 thereof. As implemented, the extracted information is either contextually or taxonomically associated. As explained by the inventors: "A simple classification system (hierarchical taxonomic system) can be established by reviewing the label descriptions on the structured data and then expanding class definitions with the use of the Knowledge Expander (KE) search engine. [...] The hierarchical taxonomic system can be used to build contextual filters and taxonomic filters which can further protect Sec-Con data and expand the value and quantity of SC data." *See* '301 Patent at 10:22-32. In practice, Sheltered Harbor systems allow for the grouping of tags using metadata or any of a number of functionally equivalent means of achieving the same result; namely, the filtering of data for inclusion in designated storage. By way of example, in the certified Dell

PowerProtect system, virtual machine tags are created in the "vSphere Client." Such virtual tags enable the enterprise to attach metadata to virtual inventory assets, making them easier to sort and search. *See* Virtual Machine User Guide at 56. Tags are grouped within categories, which can further include specific object types. *See* Virtual Machine User Guide at 56-58 (describing tag creation and protection rules). The use of tag grouping, including by the use of metadata, is an implementation of contextually or taxonomically associated data.

226. Still further, and as noted above, Sheltered Harbor compliant systems analyze (inference) content with such contextual and taxonomic filters in order to obtain the inferenced sensitive and select content. As implemented, for example, in the compliant Dell PowerProtect system, content scans are performed. *See, e.g.,* Dell Technical White Paper entitled: Zero-Trust, A Key Framework in Dell Technologies' Overall Data Protection Strategy, available at: www.delltechnologies.com/asset/en-us/products/security/industry-market/zero-trust-whitepaper.pdf (as visited October 20, 2023) (hereafter as "Zero-Trust"), at 7-9 (explaining data analytics and full replication in the data vault).

227. In view of the foregoing, and on information and belief, the Accused Instrumentalities thus comprise an apparatus which directly performs the step of inferencing said sanitized sensitive content data and select content data with (a) a content filter, (b) a contextual filter, and (c) a taxonomic filter; and obtaining an inferenced sensitive content data and an inferenced select content data therefrom.

228. The foregoing infringement on the part of Defendant has caused past and ongoing injury to Plaintiff. The amount of damages adequate to compensate for the infringement shall be determined at trial but is in no event less than a reasonable royalty from the date of first

infringement to the expiration of the '639 Patent.

229. To the extent Defendant continues, and has continued, its infringing activities noted above in an infringing manner post-notice of the '639 Patent, such infringement is necessarily willful and deliberate.

230. Each of Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

COUNT V
Knowledge and Willfulness

231. Plaintiff incorporates the above paragraphs by reference.

232. Defendant has been on actual notice of the DigitalDoors Patents since at least as early as the date it received service of this Original Complaint. In the alternative, Defendant has been on actual notice of the DigitalDoors Patents since at least September 30, 2014, by virtue of patent prosecution arguments made in the United States Patent and Trademark Office during prosecution of Defendant's own patent applications, including but not limited to applications issuing as United States Patent Nos. 8,849,716; 10,380,374; 10,482,069; and 11,379,416.

233. On information and belief, Defendant has a policy or practice of not reviewing the patents of others. Further on information and belief, Defendant instructs its employees to not review the patents of others for clearance or to assess infringement thereof. As such, Defendant has been willfully blind to the patent rights of Plaintiff.

PRAYER FOR RELIEF

WHEREFORE, DigitalDoors, Inc. respectfully requests the Court enter judgment against Defendant as follows:

A. Declaring that Defendant has infringed the Asserted Patent(s);

B. Awarding DigitalDoors, Inc. its damages suffered because of Defendant's infringement of the Asserted Patent(s);

C. Awarding DigitalDoors, Inc. its costs, reasonable attorneys' fees, expenses, and interest;

D. Granting a permanent injunction pursuant to 35 U.S.C. § 283, enjoining Defendants from further acts of infringement with respect to the Asserted Patent(s);

E. Awarding DigitalDoors, Inc. ongoing post-trial royalties for infringement of the non expired Asserted Patent(s); and

F. Granting DigitalDoors, Inc. such further relief as the Court finds appropriate.

JURY DEMAND

Plaintiff DigitalDoors, Inc. respectfully demands trial by jury, under Fed. R. Civ. P. 38.

Dated: January 1, 2025

Respectfully submitted,

/s/ Joseph J. Zito

Joseph J. Zito
DNL Zito
1250 Connecticut Ave NW, Suite 700
202-466-3500
jzito@dnlzito.com
Attorney for DigitalDoors, Inc.