

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

HID GLOBAL CORPORATION.,

Plaintiff,

v.

**VECTOR FLOW, INC. et al.,
Defendants.**

Civil Action No. 21-1769 (GBW)

**DECLARATION OF STEPHEN GRAY IN SUPPORT OF DEFENDANT VECTOR
FLOW'S CLAIM CONSTRUCTION BRIEF**

Table of Contents

I.	Introduction.....	1
II.	Qualifications.....	1
III.	Preparation of Declaration and Retention.....	2
IV.	Overview of Patents-in-Suit.....	3
V.	Definition of Person of Ordinary Skill.....	3
VI.	Legal Principles	4
VII.	Analysis.....	5
A.	“sensor” (’704, claims 11-15; ’088, claim 15).....	5
B.	“sensor data” (’704, claims 11, 13).....	10
C.	“native data representation format” (’704, claims 11, 13).....	11
D.	“individual user profiles” (’704, claim 11).....	14
E.	“rule” / “rules” (’704, claims 11, 14, 15; ’088, claims 15-17	16
F.	“visual rules” (’704, claim 11).....	17
G.	“live objects” (’704, claim 11).....	19
H.	“routing rules” (’704, claim 11).....	20
I.	“transformation rules” (’704, claim 11).....	20
J.	“physical security” (’704, claim 11; ’088, claims 15, 16)	21
K.	“single integration layer component” (’088, claim 15)	22
L.	“protocol defined trap message” (’088, claim 15).....	24
M.	“system log daemon” (’088, claim 15)	26
N.	“physical security state engine” (’088, claim 15)	27
O.	“virtual objects” (’088, claims 15, 16).....	28
P.	“reference” / “references” (’088, claim 15)	30

I, Stephen Gray, under penalty of perjury, declare and state as follows:

I. INTRODUCTION

1. I have been retained as an expert witness in the above-captioned case by Defendants. The following declaration is based on my personal knowledge and, if called as a witness, I could and would testify competently thereto.

2. I understand that HID Global Corporation (“HID”) has asserted two patents in this matter: U.S. Patent No. 8,234,704 (the “’704 Patent” or “’704”) and U.S. Patent No. 9,111,088 (the “’088 Patent” or “’088”) (collectively, the “Asserted Patents”). I understand that these patents are involved in claim construction proceedings.

3. For this declaration, I have been asked to analyze and opine on proposed claim constructions for terms disputed in this matter, and to respond to the declaration of Dr. Mark Jones (“Jones Declaration”). This declaration sets forth my opinions and provides the bases for my opinions regarding the meaning of the disputed terms.

II. QUALIFICATIONS

4. I have over 40 years of experience in the computer, software, and communications industries. My background and professional experience include systems and software architecture, design, and development. I have expertise in computing platform architecture, design, implementation, and integration, including relational database design in networking environments. My curriculum vitae, which describes in additional detail my experience and qualifications, is attached as Appendix 1.

5. For example, since the mid-1970s, I have designed, developed, and deployed computing systems and products that operate in server, client, and graphical environments. I have acquired expertise in the areas of distributed computing architecture and design, graphical user

interfaces, operating systems, distributed data management, local area and wide area networks, and various programming languages used in the development of those systems and products.

6. In the 1980s, for example, I worked at Xerox Corporation directing the architecture, design, development, testing, product transfer, and engineering of six products for electronic page printers connected to IBM's mainframes (MVS, VSE, VM), DEC VAX (VMS) and IBM's PCs (DOS). I continued as a consultant for Xerox, including in the mid-1990s. One of my assignments was to develop strategies for data management among network attached office products. One of the distributed data management strategies that I delivered provided end user visibility into printer queues supporting distributed network printers. Another distributed data management strategy that I delivered provided network operations distributed job management control.

7. In the early 2000s, as Chief Technology Officer for Networld Exchange Inc., I was responsible for the design, development and deployment of a suite of products that delivered eCommerce functions. These functions were provided over the Internet and included product catalog information display, purchase and/or purchase order creation, order delivery to fulfillment systems and order status reporting. The products that I had responsibility for performed numerous operations, including data synchronization, on data distributed among geographically dispersed computing entities.

8. Much of my career has been spent as a software development professional. I have had numerous occasions to write, modify, analyze, and otherwise review bodies of source code. I have analyzed source code written in several variants of C, SQL, COBOL, PHP, RPG, variants of Basic, Java, Perl, several Assembler languages, and others.

III. PREPARATION OF DECLARATION AND RETENTION

9. In forming my opinions, I have reviewed and considered the patents, prosecution histories, the parties' claim construction charts, extrinsic evidence, and any other materials cited

herein. I have also relied on my professional and academic experience. I reserve the right to consider additional materials as I become aware of them and to revise my opinions accordingly.

10. I have been retained as an expert or consultant in a variety of matters. A list of those matters from the past five years is provided in Appendix 1.

11. I am being compensated for my work in connection with this litigation at my customary rate of \$450 per hour, plus reimbursement for expenses. No part of my compensation is dependent upon the outcome of this case or any issue in it.

IV. OVERVIEW OF PATENTS-IN-SUIT

12. I understand that HID has asserted the following claims against Vector Flow: claims 11-15 of the '704 Patent and claims 15-17, 19, and 20 of the '088 Patent (collectively, the "Asserted Claims"). They both "relate generally to physical security systems, and more specifically to a system for integrating disparate security systems using a rules-based policy engine and normalized data format." '704, 1:24-27; '088, 1:23-26. Both patents share some figures and a substantial portion of the specification.

13. The specification describes an embodiment of aspects of the Asserted Patents as follows: "FIG. 5 is a flowchart that illustrates a method of creating rules and processing source security data in an integrated physical security management process, under an embodiment." '704, 11:52-55; '088, 13:17-20. Additional relevant portions of the specifications are discussed below where applicable and relevant to the issues in dispute.

V. DEFINITION OF PERSON OF ORDINARY SKILL

14. Unless otherwise specified, when I refer to a person of ordinary skill in the art or POSITA, I am referring to someone with the level of knowledge and understanding described in paragraph 26 of the Jones Declaration. I note that the analysis and opinions in my declaration

would not change if a slightly different description of the person of ordinary skill in the art was used, such as somewhat more or less education and/or experience in the relevant field.

15. I note that I was at least a POSITA as of the priority dates of the asserted patents, and I continue to be at least a person of ordinary skill in the art. The analysis and opinions regarding the patents that I provide in this declaration have been based on the perspective of a POSITA as of the relevant times, unless otherwise noted.

VI. LEGAL PRINCIPLES

16. I have been informed that patent claim terms should be interpreted consistent with the understanding that a person of ordinary skill in the art would have had at the time of the claimed invention. I have been informed that the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. I have been informed that the prosecution history can often inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be.

17. I have been informed that a claim must, when read considering the patent's specification and the prosecution history, inform a person of ordinary skill in the art about the scope of the invention, such that the person of ordinary skill in the art knows the scope with reasonable certainty. I have been informed that a claim is *indefinite* when, read considering the specification delineating the patent, and the prosecution history, the claim fails to inform, with reasonable certainty, those skilled in the art about the scope of the claimed invention.

18. I have also reviewed the principles of law stated in paragraphs 15-20 of the Jones Declaration and developed my opinions stated herein consistent with those principles.

VII. ANALYSIS

A. “sensor” (’704, claims 11-15; ’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a device that responds to a physical stimulus and transmits a resulting signal <i>Alternatively:</i> A device that responds to a physical stimulus and makes available resulting information.

19. In my opinion, the patents and claims use the term “sensor” consistent with its relevant customary meaning in the field that a POSITA would have understood, which is a device that responds to a physical stimulus and transmits a resulting signal.

20. The patents describe sensors consistent with this customary meaning. The specification describes, for example:

Facility **102** may represent a house or office building, or any other type of structure that contains some level of physical security infrastructure. The alarm and monitor elements of the physical security systems represent various access control, monitoring, surveillance, sensor, or other asset protection mechanisms that may be employed throughout the facility. These can be independent elements that are configured to detect and report different types of events, such as fire, gas leaks, intrusion, computer hacking, physical proximity, and any other similar type of event. Such systems can thus be used to control personnel access within a facility and to detect unauthorized access by inside or outside personnel, as well as to detect natural events, such as fires, earthquakes, etc. Detection of any such event can be used to alert proper officials and/or automatically invoke protection mechanisms, such physical shutdown, backup of computers, turning on lights, and so on.

’704, 4:9-25; ’088, 4:28-44 (underlining added).

21. This passage describes multiple different types of items: sensors, as well as other types of access control, monitoring, surveillance, or other asset protection mechanisms. Other passages of the specification provide a similar distinction: “The alarm and monitor elements of the

physical security systems represent various access control, monitoring, surveillance, sensor, or other asset protection mechanisms that may be employed throughout the facility.” ’704, 4:11-15; ’088, 4:30-34 (underlining added).

22. The specification thus makes clear to a POSITA that not all monitoring and surveillance systems are considered “sensors” within the context of the claimed invention.

23. The specification further specifically discusses “physical sensors,” confirming that the sensors contemplated by the proposed invention are customary sensors that respond to physical stimuli and transmit a resulting signal conveying sensor data. “The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities, such as facilities 102 and 103 in FIG. 1A, block 506.” ’704, 11:63-66, Fig. 5 (item 506: “collect data and alarm events from physical sensors, monitors and alarms”) (underlining added); ’088, 13:28-31, Fig. 5 (item 506). Again, the specification here distinguishes “sensors” versus monitors and alarms.

24. Claim 3 of the ’704 patent and claim 20 of the ’088 patent reinforce the same meaning. Claim 3 of the ’704 patent depends from claim 2, which depends from claim 1, and states that the “plurality of sensors are selected from the group consisting of: proximity alarms, infrared detectors, motion sensors, smoke detectors, bar code readers, and biometric sensors,” indicating that all of these items are considered “sensors” within the meaning of the claims. Claim 20 of the ’088 patent depends from claim 15 and recites that “the disparate security devices are selected from the group consisting of: proximity alarms, infrared detectors, motion sensors, smoke detectors, bar code readers, and biometric sensors.” A POSITA would have understood that each of these items recited in these claims is a device that responds to a physical stimulus (for example, physical proximity, light, motion, smoke, a bar code pattern detected through light, and biometric stimuli from a human such as fingerprints or an eye scan image) and transmits a resulting signal.

25. Tellingly, while “computer hacking” is mentioned in the specifications as a type of monitoring or surveillance mechanism, computer hacking is conspicuously not included in these lists of sensors in these claims. A POSITA would have understood that software that detects computer hacking (or a device programmed with software that detects computer hacking) is distinct from a “sensor” within the meaning of the patents.

26. As the word “sensor” indicates, the meaning of the term in the relevant context is similar to how humans sense their physical environment with their senses. Consider an example in the context of the physical security of a building. A human, such as a security guard, can use their senses to see and hear intruders or smell smoke. The person’s eyes, ears, and nose act as sensors that respond to physical stimuli from the environment. The sense organs transmit signals to the brain, resulting in visual, audible, and olfactory signals. In the context of the patents, a “sensor” is a device that performs an analogous function as human sense organs: responding to a physical stimulus and transmitting a resulting signal.

27. The same customary meaning of the term “sensor” provided by the patents was also reflected in dictionaries. The following are some illustrative definitions showing this meaning.

- “a device that responds to a physical stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse (as for measurement or operating a control).” Ex. 16 (Merriam-Webster’s Collegiate Dictionary (11th ed. 2004)).
- “A device that responds to a physical stimulus (such as heat and light) and transmits a resulting signal.” Ex. 17 (IEEE Standard Dictionary of Electrical and Electronics Terms (6th ed. 1996)).
- “An electronic device that converts into an electrical signal some physical property of its environment – for example temperature, pressure, motion, light intensity, oxygen concentration or acidity.” Ex. 18 (The Penguin Concise Dictionary of Computing (2003)).

28. The Jones Declaration states: “a POSITA reading the claims in the context of the specification would understand that a ‘sensor’ is a device configured to detect information.” Jones Declaration, ¶ 30. This statement does not provide an accurate definition of the term “sensor” in

the context of these patents. Many devices configured to detect information of a non-physical nature or a logical nature, such as using computer software to detect electronic information, would not be considered a “sensor” as recited in the claims. For example, as discussed above, the specifications mention “computer hacking” as one form of monitoring or surveillance but does not identify any device that detects information about computer hacking as a “sensor.” Software that detects computer hacking (or a device programmed with software that detects computer hacking), or software that detects other non-physical electronic information such as detecting computer viruses or detecting information that input by a user, or that merely detects logical information unrelated to the physical environment such as in data processing, does not provide a “sensor” within the meaning of the patents.

29. The Jones Declaration posits that sensors “need not necessarily transmit a resulting signal.” Jones Declaration, ¶ 35. I respectfully disagree with the suggestion that the term “sensor” in the context of these patents and claims encompasses devices that cannot transmit a resulting signal. The claims at issue, and the descriptions in the patent specification, recite and describe that “sensor data” is transmitted from the sensors. For example: “The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities, such as facilities 102 and 103 in FIG. 1A, block 506.” ’704, 11:63-66, Fig. 5 (item 506: “collect data and alarm events from physical sensors, monitors and alarms”) (underlining added); ’088, 13:28-31, Fig. 5 (item 506). No example is provided in the patents that a POSITA would understand to be a “sensor” that does not transmit a resulting signal after sensing physical stimuli. A POSITA would have understood that each “sensor” contemplated by the patents has circuitry or other internal components that transmit a resulting signal based on the physical stimuli sensed from the environment. The transmission of the signal can be immediate either within the sensor or external to the signal, or an external device could also poll or request the sensor to transmit the

resulting signal. The point is that a sensor, in the relevant context, makes available information resulting from responding to the physical stimulus and is designed to transmit that resulting signal.

30. In fact, even the one dictionary definition of “sensor” cited in the Jones Declaration defines the term “sensor” as an item that “serves to sense . . . and respond,” indicating that a “sensor” responds (that is, transmits a resulting signal) based on what it senses. Jones Declaration, ¶ 33 (citing Wiley Electrical & Electronics Engineering Dictionary (2004)) (underlining added).

31. The Jones Declaration posits that “sensors can respond to non-physical stimuli.” Jones Declaration, ¶ 35. I respectfully disagree that the term “sensor” in the context of these patents and claims encompasses devices that respond to non-physical stimuli. The Jones Declaration points to “IT intrusion” and “computer hacking,” but tellingly the patents never specifically describe or claim IT intrusion or computer hacking as being detected by a sensor. Instead, a POSITA would understand that other access control, monitoring, and/or surveillance systems using software would detect information about IT intrusion and computer hacking, as discussed previously.

32. The Jones Declaration points to its one cited dictionary definition mentioning “time” sensors as a purported example of responding to a non-physical stimuli. Jones Declaration, ¶ 35. However, the Jones Declaration does not identify any disclosure of a purported “time sensor” in these patents. In the context of these patents and claims, a POSITA would not have understood that a device that does not respond to physical stimuli would be a “sensor” within the meaning of the claims. Moreover, a sensor could effectively measure the passage of time by responding to physical stimuli, insofar as the passage of time is coextensive with and can be determined with reference to changes in the physical world.

B. “sensor data” (’704, claims 11, 13)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	the data transmitted by a sensor in response to a physical stimulus <i>Alternatively:</i> The data made available by a sensor in response to a physical stimulus.

33. In my opinion, a POSITA would have understood the term “sensor data” in claims 11 and 13 of the ’704 patent to mean the data transmitted by a sensor in response to a physical stimulus. The meaning of “sensor data” here is consistent with the meaning of the term “sensor” as discussed in the previous section.

34. Claim 11 recites that “sensor data” is output from each sensor: “accepting sensor data from each security sensor . . . wherein the sensor data from each security sensor is embodied in a native data representation format.” ’704, claim 11. Claim 13 further recites: “The method of claim 11 further comprising converting the native data representation format for each security sensor into XML (Extensible Markup Language) format, and wherein the native data representation format encompasses native sensor data including text data and binary data represented in a proprietary format, and wherein the native sensor data includes at least one of a command or sensor state information.” *Id.*, claim 13.

35. The specification similarly describes that data is transmitted by the “physical sensors” that respond to physical stimuli: “The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities.” ’704, 11:63-66, Fig 5 (item 506: “collect data and alarm events from physical sensors, monitors and alarms”).

36. As discussed in the previous section, a POSITA would have understood that the sensors contemplated by the patents are devices that respond to a physical stimulus (for example, physical proximity, light, motion, smoke, a bar code pattern detected through light, and biometric

stimuli from a human such as fingerprints or an eye scan image) and transmit a resulting signal. The purpose of these sensors, in context, would be understood to transmit data that would be collected based on whatever was detected. For example, if the sensor detects motion or smoke or a bar code, data is transmitted by the sensor as a result.

37. The Jones Declaration states:

Vector Flow's proposed construction is too narrow because the sensor data includes more than "data transmitted by a sensor in response to a physical stimulus." For example, dependent claim 13 of the '704 Patent recites that the "sensor data" includes "text data and binary data represented in a proprietary format," as well as "a command or sensor state information." Vector Flow's proposed construction seemingly excludes these embodiments."

Jones Declaration, ¶ 35.

38. I respectfully disagree. Claim 13 states in relevant part: "wherein the native data representation format encompasses native sensor data including text data and binary data represented in a proprietary format, and wherein the native sensor data includes at least one of a command or sensor state information." '704, claim 13. Nothing in this statement indicates that the sensor data is not transmitted in response to a physical stimulus. Nothing in this claim is excluded by the meaning of sensor data taught by the specification and understood in context, namely the data transmitted by a sensor in response to a physical stimulus. The sensor data transmitted in response to a physical stimulus may include command or sensor state information.

C. "native data representation format" ('704, claims 11, 13)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	the original format of the data transmitted by a sensor in response to a physical stimulus. <i>Alternatively:</i>

	The original format of the data made available by a sensor in response to a physical stimulus. <i>Or:</i> A data format that is built into a sensor.
--	---

39. In my opinion, the term “native data representation format” in the context of claims 11 and 13 of the ’704 patent would have been understood by a POSITA to refer to the original format of the data transmitted by a sensor in response to a physical stimulus, *e.g.*, a data format that is built into a particular sensor.

40. This meaning flows from the patent and is consistent with the customary meaning of a “native” data format in the field. The claim language recites: “the sensor data from each security sensor is embodied in a native data representation format of each respective manufacturer of the plurality of manufacturers.” ’704, claim 11. Claim 13 further references “the native data representation format for each security sensor.” *Id.*, claim 13. I have opined on the terms “sensor” and “sensor data” above. The “native data representation format” in the claims refers to sensor data output from a sensor. The question, however, is the proper meaning of the “native” data representation format, as opposed to data that would not be considered to be in a “native” format.

41. The specification discusses that data is received from devices and systems “in their native, proprietary format.” ’704, 7:37-52. It describes that “data and events are received in the native format of the individual systems, such as lighting/control devices, access readers, door controllers, infrared sensors, card readers, and personnel control agents.” *Id.*, 9:59-10:2. When data is collected from physical sensors, the “data is collected in native format” and then normalized into a common format: “The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities, such as facilities 102 and 103 in FIG. 1A, block 506. This data is collected in native format and then aggregated and normalized in

accordance with defined data mapping and translation schemes, block 508. This formats the data and events into a format to enable processing by the defined rules.” *Id.*, 11:52-12:3.

42. Based on these descriptions, a POSITA would have understood that the patents use the term “native data representation format” consistent with its customary technical meaning in the field, referring to a data format that is built into the system, thus providing the original format of data that originates from that system.

43. Technical dictionaries likewise reflect the meaning that a “native” format is the “original form” of data, such as a “native file format” that “an application uses internally to process data.” The following definitions illustrate this meaning.

Native: “Of, pertaining to, or characteristic of something that is in its original form. For example, many applications are able to work with files in a number of formats; the format the application uses internally is its native file format. Files in other formats must be converted to the application’s native format before they can be processed by the application.” Ex. 19 (Microsoft Computer Dictionary, 4th Ed.) (1999)
--

Native file format: “The format an application uses internally to process data. The application must convert files in other formats to the native format before it can work with them. For example, a word processor might recognize text files in ASCII text format, but it will convert them to its own native format before it displays them.” Ex. 19 (Microsoft Computer Dictionary, 4th Ed.) (1999)
--

44. The Jones Declaration identifies one dictionary definition from the IEEE Standard Dictionary of Electrical and Electronics Terms (1996) that is consistent with this meaning, identifying the term “native data type” with the meaning of “[a] data type that is built into a software or hardware system.” Jones Declaration, ¶ 40. In my opinion, this meaning is another way of identifying essentially the same meaning of the “native” data representation format for a

sensor in context of the claims here, referring to a data format that is the original format of data output by the sensor, because that data format is built into the sensor by the manufacturer of the sensor.

45. The Jones Declaration states: “I disagree with Vector Flow’s inclusion of ‘original format’ in its proposed construction. It is unclear what Vector Flow means by ‘original format,’ but assuming Vector Flow means the format of the sensor data produced by the sensor, then this part of its construction is, at best, unnecessarily duplicative.” Jones Declaration, ¶ 41. The declaration does not appear to dispute that the claimed “native” format refers to “the format of the sensor data produced by the sensor,” or that this “native” format is the original format of data output by the sensor or the format that is built into the sensor.

D. “individual user profiles” (’704, claim 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a profile corresponding to an individual user

46. In my opinion, a POSITA would have understood the term “individual user profile” in claim 11 of the ’704 patent to refer to a profile corresponding to an individual user.

47. This meaning is evident from the claim language of claim 11, which recites “defining individual user profiles and their respective access privileges and credentials in the system.” A POSITA would understand from the claim language that the claim language is dealing with user profiles for individual users—humans who are users—who have access privileges and credentials.

48. The specification confirms this meaning that “individual user profile” refers to a profile corresponding to an individual user. It describes as follows, that the profile for a particular

individual can be used to generate “unique” access credentials using an “exclusive” mapping with a particular individual’s profile:

In one embodiment, the integrated physical security management process 118 includes a normalization process that normalizes of disparate security systems data to a standard data format, for example, access control and alarm data. It also includes processes to generate unique physical access credentials to provide an exclusive mapping between an individual’s profile (job, department, location, and so on) and an organization’s spatial hierarchy of its global physical security system deployments (doors, buildings, lockers, safes, and so on). For personnel control, the integrated physical security management process 118 is configured to generate unique physical access credentials based on individual profiles to automatically assign credentials across multiple global physical security systems to overcome certain limitations (e.g., memory constraints) of standard access control systems.

’704, 5:1-17 (underlining added).

49. The specification reiterates:

The disclosed system also provides processes and systems to generate unique physical access credentials for exclusive mapping between an individual's profile (job, department, location, etc) and an organizations spatial hierarchy of its global physical security system deployments (doors, buildings, etc), and generates unique access credentials based on individual profiles and automatic assignment across multiple physical security systems overcoming certain hardware/software limitations of standard access control system/hardware.

’704, 18:29-38 (underlining added).

50. The Jones Declaration states: “Vector Flow seeks to narrow the scope of the phrase such that a single individual user corresponds to a specific profile.” Jones Declaration, ¶ 51. I respectfully disagree. The plain claim language recites “individual user profiles,” and the specification describes how this language refers to a profile corresponding to an individual user, as discussed above. A POSITA would have understood that the claim language and specification contemplate that a single individual user corresponds to a specific profile.

E. “rule” / “rules” (’704, claims 11, 14, 15; ’088, claims 15-17)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system

51. In my opinion, a POSITA would have understood the term “rule” in the patents to be defined by the specification as the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system.

52. The specification provides this meaning by explaining, as a matter of definition, what “rules are” in the context of the patents: “Rules are the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system.” ’704, 11:48-50, ’088, 13:13-15 (same). The patents reiterate: “Rules are the actual and lowest level combination of Condition-Action sequences that are applied to the data objects passing through the process.” ’704, 13:67-14:2; ’088, 20:19-21 (same). These statements would be understood by a POSITA to define what “rules” mean in the context of the disclosure.

53. These definitional statements contrast with examples of features that the specifications described that rules “can” optionally have. For example, a “rule can have multiple actions defined for it,” “rules can cause any number of internal or external actions to be taken,” “the order of execution of rules can be changed,” among other things. ’704, 16:3-5, 12:4-6, 14:6-9 (underlining added); ’088, 22:23-25, 13:36-38, 20:25-26.

54. The Jones Declaration states: “Vector Flow’s proposed construction contradicts the claim language, at least because claim 11 of the ’704 Patent already recites that the ‘rules compris[e] condition-action sequences.’” Jones Declaration, ¶ 68. I respectfully disagree. Vector Flow’s proposed construction matches the definition in the specifications, which defines that rules are the actual lowest level combination of Condition-Action that is applied to the data objects

processed by the system. This meaning does not contradict the claim language. In fact, it is perfectly consistent with the claim language. Rules are the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system, and as recited in claim 11 of the '704 patent, the rules comprise condition-action sequences.

55. The Jones Declaration states: “In addition, in my opinion, the above passages do not provide an express definition of the terms ‘rule’ and ‘rules,’ which, as discussed above, are recited throughout the Asserted Claims in different variations. Rather, the above passages provide generalized introductions to the nature of the ‘rules’ and how they are used by the system in at least one embodiment, but are not clear definitions of the terms ‘rule’ and ‘rules,’ nor do they clearly express an intent to redefine the terms.” Jones Declaration, ¶ 69. I respectfully disagree. The definitional statements in the specifications do not state that they are merely describing example embodiments. They are definitional as to what “rules are” in the context of the patents.

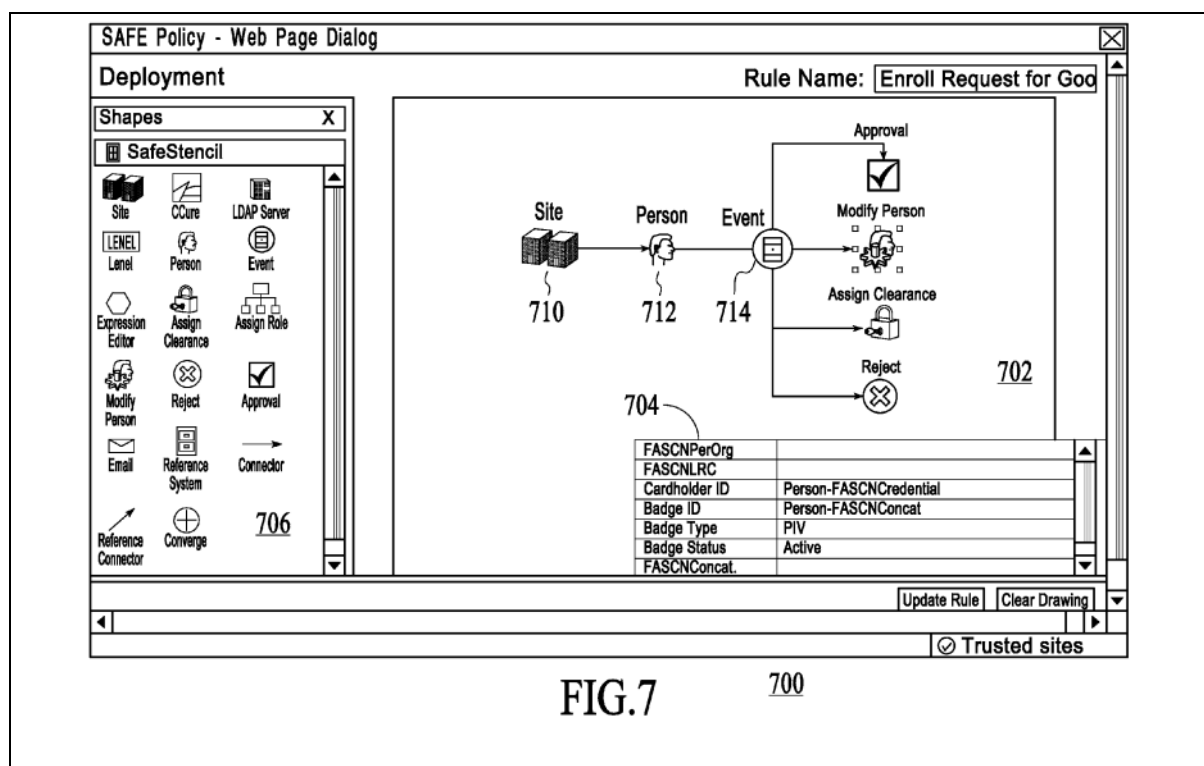
F. “visual rules” ('704, claim 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a rule that is visually defined and depicted in a display area by placing icons and connectors in appropriate relationships to one another

56. In my opinion, the term “visual rules” in the claims and specification of the '704 patent is not used with a commonly understood customary meaning in the field that a POSITA would have understood. I have performed research online, as well as considered my own decades of experience, to confirm the basis for this opinion. A POSITA would have understood that the term “visual rules” is a coined term used with its own meaning as defined by the patents.

57. The specification teaches the creation of a “visual rule,” as a rule that is visually defined by placing icons and connectors in appropriate relationships to one another. Specifically, the specification explains that Figure 7 depicts a visual policy editor used to construct visual rules,

comprising a “main display area 702” that “allows a user to visually define a rule by placing icons and connectors in appropriate relationships to one another.” ’704, 17:3-6, Fig. 7, 2:53-55 (underlining added). The specification further similarly describes that visual rules are “created visually through the use of a stencil of object shapes that represent physical systems, data flow and processes.” *Id.*, 16:43-45 (underlining added). In a user interface, a “rule is created by dragging and dropping drawing objects on to the map and interconnecting them to create rules.” *Id.*, 16:53-55 (underlining added); *see also id.*, 11:34-36 (rules are “created using a visual policy editor using drag and drop graphical user interface techniques” involving the “interconnection of rule objects....”). Figure 7 of the patent depicts visual rules, showing the icons used to depict items 710, 712, and 714 in spatial relationship with one another using connectors (arrows) to construct the rule “Enroll Request ...”. *See id.*, Fig. 7. Figure 7 is reproduced below for reference:



58. The Jones Declaration at paragraph 72 further notes that the specification states: “visual rule objects contain attributes that define their spatial relationship to other building blocks that are used to represent normalized systems, data and processes.” ’704, 11:10-13. This description is consistent with the descriptions noted above. As shown in Figure 7 and the corresponding textual description discussed above, visual rules are visually defined and depicted in a display area by placing icons and connectors in appropriate relationships to one another. The visual rules, as created, may involve visual rule objects that contain attributes that define their spatial relationship to other building blocks that are used to represent normalized systems, data and processes.

G. “live objects” (’704, claim 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
Plain and ordinary meaning; “stencil objects.”	Stencil shapes that are used to represent normalized systems, data and processes.

59. In my opinion, the term “live objects” in the claims and specification of the ’704 patent is not used with a commonly understood customary meaning in the field that a POSITA would have understood. I have performed research online, as well as considered my own decades of experience, to confirm the basis for this opinion. A POSITA would have understood that the term “live objects” is a coined term used with its own meaning as defined by the patents.

60. Specifically, the term “live objects” is defined by the specification as follows: “The visual rule objects contain attributes that define their spatial relationship to other building blocks that are used to represent normalized systems, data and processes. Such building blocks are also referred to as stencil shapes or live objects.” ’704, 11:10-14 (underlining added). Based on this description, a POSITA would understand that “live objects” are stencil shapes, and particularly stencil shapes that are used to represent normalized systems, data and processes.

H. “routing rules” (’704, claim 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a rule that controls the flow of data between different connected systems

I. “transformation rules” (’704, claim 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a rule that defines and maintains the transformational mapping of data and events between different connected systems

61. The meaning of the claim term “rules” is addressed above. The ’704 patent and claims further specify particular types of rules. Two types of rules are addressed here. In my opinion, each of the terms “routing rules,” “transformation rules” and “transformation and routing rules” in the claims and specification of the ’704 patent is not used with a commonly understood customary meaning in the field that a POSITA would have understood. I have performed research online, as well as considered my own decades of experience, to confirm the basis for this opinion. A POSITA would have understood that the terms “transformation rules” and “routing rules” (in the context of “transformation and routing rules” as recited in claim 11 of the ’704 patent) are coined terms used with their own meaning as defined by the patents.

62. The meaning of these coined terms is evident from the specification of the ’704 patent. The specification describes that a “transformation and routing module” “defines and maintains the transformational mapping of data and events between the different connected systems” (which a POSITA would understand to correspond to transformation rules), and also “controls the flow of the data between systems through rules based routing as defined by certain physical security policy process[es], states, and actions....” (which a POSITA would understand

to correspond to routing rules). '704, 9:19-24 (underlining added). A POSITA would have understood, in view of these disclosures, that transformation rules and routing rules are distinct categories of rules.

J. “physical security” ('704, claim 11; '088, claims 15, 16)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	security of a physical site

63. A POSITA would have understood that the term “physical security” as used in the patents refers to the security of a physical site, such as by physically monitoring and controlling persons and events in a building. The concept of “physical security” would be understood in contrast with non-physical security measures, such as information technology (IT) security measures. For example, software that detects computer network hackers performs a security function, but it is not physical security in this context.

64. The specifications describe this meaning:

Physical security systems include equipment and processes that implement physical security measures for incidents, access control, monitoring systems, lighting, security, audits, inspection, facility management, building automation, and the like. Almost all businesses, large commercial and government facilities, and many homes utilize physical security systems to alert owners and operators about potentially harmful activities such as intrusion, theft, fire, flooding, gas leaks, and so on.

'704, 1:31-39; '088, 1:30-38.

65. The dictionary definitions of “physical security” cited in paragraph 95 of the Jones Declaration are consistent with this meaning. Those definitions are reproduced below.

	single database. Also called physical security Measures such as locking the enclosure or housing of a device, restricting entry into certain areas, or using tamper-evident materials, which help to physically avoid security breaches.
	physical security Protection of system resources from physical access, tampering, and destruction, such as through the use of barriers, locks, seals, and intrusion detection systems.

66. Paragraph 96 of the Jones Declaration states: “Vector Flow’s limitation that ‘security’ must be directed to a physical ‘site’ excludes security that may be generally related to a physical site, but does not rise to the level of specificity of ‘security of a physical site.’” I respectfully disagree with the suggestion that all “security that may be generally related to a physical site” would be understood to fall within the limitation of “physical security” as recited in the claims. Various security measures and mechanisms “generally related to a physical site” may include non-physical security measures, such as computer network hacking and malware/virus detection security for the servers at a particular physical site, that would not be understood by a POSITA to be “physical security” in the context of the claimed invention here.

K. “single integration layer component” (’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	Indefinite

67. In my opinion, the ’088 patent fails to provide a POSITA with reasonable certainty as to the meaning of the term “single integration layer component.”

68. This term “single integration layer component” did not have a customary meaning in the field, based on my experience and research. It is a term coined by the patent. However, the specification fails to provide adequate guidance on the scope and meaning of the term so as to

inform a POSITA with reasonable certainty as to what would fall inside of, and outside of, the scope of this claim term.

69. The claim language is ambiguous as whether “a single integration layer component” refers to (1) a single component in any integration layer or (2) a component in a single integration layer. The specification never uses the word “single” in this context. The only uses of the word “single” in the specification are irrelevant mentions on “a single building” and “a single vendor” in the background section. ’088, 1:54-63. There is no discussion or teaching of what would constitute a “single” component in an integration layer, or a “single” integration layer, as opposed to multiple (non-single) components or layers. The specification does not differentiate “single” versus “non-single” in this context. The specification discusses an “integration layer” but provides the discussion only in high-level functional terms that do not provide reasonable certainty as to what would fall inside of, or outside of, an integration layer. For example:

An integration layer contains agents and adapters with built-in intelligence for multiple physical security systems and supports extensibility through mapping of application protocols, command and data 152 formats for integration with new and emerging physical security systems. It also normalizes the communication data, commands and events from the disparate physical security systems to a common standard format. . . .

All of the disparate data is routed to the integration layer of the system orchestration framework, which is configurable to support the multiple physical media, network protocol and data formats that can be used to integrate with various systems.

’088, 7:59-66, 11:61-65.

70. These descriptions generally mention an “integration layer” but do not provide meaningful guidance as to the boundaries of what would be considered to fall inside or outside of an integration layer.

71. Further, the specification states an open-ended definition of the term “component” as follows: “Throughout the description, the terms, ‘module,’ ‘component,’ and ‘process’ may be

used interchangeably to mean an [sic] computer program, routine, or subroutine that is executed on any of the server and/or client computers of FIG. 1A, and may be implemented as software, firmware, or programmed hardware.” *Id.*, 6:45-50.

72. Taken as a whole, the descriptions fail to provide meaningful guidance on the metes and bounds of the claimed “single integration layer component.” A POSITA would not have found the specification to provide reasonable certainty as to the scope of this claim language.

L. “protocol defined trap message” (’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	an unsolicited alert message defined by Simple Network Management Protocol

73. The ’088 patent specification describes the use of a Simple Network Management Protocol (“SNMP”) trap message. A “trap” message is well-known and well-understood in the context of SNMP, and would have been well-known to a POSITA. I note that the definition of a POSITA in paragraph 26 of the Jones Declaration includes experience in distributed computer systems, which would entail familiarity with SNMP as a very well-known network management protocol. A “trap” message refers to an unsolicited alert message as defined by the protocol. This meaning is reflected in the source documentation that defines SNMP. SNMP is described in RFC 1157, “A Simple Network Management Protocol” (1990), available online at <https://www.rfc-editor.org/rfc/rfc1157>. The documentation defines “traps” as “unsolicited messages” that operate consistent with the network monitoring strategy and design of SNMP: “The strategy implicit in the SNMP is that the monitoring of network state at any significant level of detail is accomplished primarily by polling for appropriate information on the part of the monitoring center(s). A limited number of unsolicited messages (traps) guide the timing and focus of the polling.” RFC 1157, §

3.2.3. The SNMP trap message is “unsolicited” as its purpose is to provide an unsolicited notification that a certain error, harm, or other condition has occurred.

74. The '088 patent uses the concept of an SNMP trap message with the same meaning: “SNMP Alarm Event (Trap): The following example defines an alarm (Trap in SNMP terminology) which is generated by a network device (system or application) containing details in the objects defined in it.” '088, 15:61-16:10 (underlining added). The specification also provides an example of “an SNMP high temperature trap,” which a POSITA would understand to be an SNMP trap message that is caused by high temperature. '088, 14:39-40 (underlining added). The specification does not teach any examples of any non-SNMP “trap” message. In context, where claim 11 of the recites “wherein the alarm event messages are generated by a protocol defined trap message,” a POSITA would have understood that the “protocol defined trap message” refers to an SNMP trap message, which is an unsolicited alert message defined by Simple Network Management Protocol.

75. The Jones Declaration at paragraph 111 states: “POSITAs understand that this term includes a protocol defined message associated with an exception that occurs in software.” I respectfully disagree with the suggestion that the term “protocol defined trap message” as described and claimed in the '088 patent would have been understood to encompass all protocol defined messages associated with an exception that occurs in software. Many different messages defined by non-SNMP protocols associated with exceptions that occur in software were known to exist, that would not have been considered a “trap” message in context, such as various types of error messages that occur in a wide variety of software applications as defined by various different protocols.

M. “system log daemon” (’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a server process that provides a message logging facility for systems

76. The “system log daemon” in the ’088 patent would be understood by a POSITA to be a server process that provides a message logging facility for systems. The ’088 specification describes “syslog” (system log) as follows: “Syslog is a method to collect messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Network vendor’s devices can send their log messages to a SYSLOG service.” ’088, 16:16-20 (underlining added). This passage provides a clear definitional teaching as to what “Syslog is . . .” in the context of the patent. That definition makes clear that the system log daemon is a “server” process, using a “syslog server.” It also makes clear that the syslog daemon, as the word “log” indicates, is a message logging facility (collecting messages from devices, such as aggregating logs and alerts sent in messages).

77. The patent specification also describes in detail examples of messages sent to a system log daemon, which clearly shows the syslog daemon being run on a server, as indicated by the “server” identification in each logged item. *Id.*, 16:22-44.

78. The claim language is consistent with “system log daemon” being a server process as described in the specification. Claim 15 recites “extracting physical security data and events from network traffic and the security components to build a continually updated security state of the entire system through alarm event messages generated by network resources, wherein . . . a system log daemon process aggregates the alarm event messages.” ’088, claim 15 (underlining added). The system log daemon processes alarm event messages generated remotely, that is, by network resources.

79. The Jones Declaration states in paragraph 116: “In my opinion, the plain and ordinary meaning of ‘system log daemon’ includes within its scope all of the embodiments and definitions described above, and is not limited to only a ‘server process’ and only message logging for a ‘system,’ as Vector Flow proposes in its construction.” I respectfully disagree. I note that the Jones Declaration effectively reads out the “daemon” limitation from the claim. A POSITA would have clearly understood from the description in the specification that the “system log daemon” recited in the claims refers to a process implemented at a server for collecting or logging messages. With respect to the term “system,” the Jones Declaration does not identify any inaccuracy in that meaning, which is consistent with the meaning taught by the patent and as understood by a POSITA with experience in distributed computing.

N. “physical security state engine” (’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	a real-time, high speed repository and access interface to all the security states defined in the system

80. In my opinion, the term “physical security state engine” in claim 15 and the specification of the ’088 patent is not used with a commonly understood customary meaning in the field that a POSITA would have understood. I have performed research online, as well as considered my own decades of experience, to confirm the basis for this opinion. A POSITA would have understood that the term “physical security state engine” is a coined term used with its own meaning as defined by the patents.

81. The only place that this term appears in the specification is in the following sentence: “The physical security state engine 326 within the PSS module 302 is the real-time, high speed repository and access interface to all the security states defined in the system.” ’088, 10:52-56 (underlining added). A POSITA would have understood that this sentence defines the meaning

of this coined term as used in the patent, since no other description is provided with the use of this term.

O. “virtual objects” (’088, claims 15, 16)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	indefinite; <i>Alternatively:</i> a visual depiction of an object that is not real

82. In my opinion, the specification and surrounding context of term “virtual objects” in claims 15 and 16 of the ’088 patent does not provide reasonable certainty as to the claim scope, and specifically the patent fails to provide sufficient guidance to a POSITA as to how “virtual objects” differ from “objects.”

83. The claim language first recites “objects” that are not recited as “virtual objects.” For example, claim 15 recites “defining a first plurality of objects representing actors, facilities, physical security states, and network resources . . .,” “defining a second plurality of objects representing actions, conditions and references . . .,” and “constructing a rule from the first plurality of objects and second plurality of objects through connectors that dictate process flow by the first and second plurality of objects.” These uses set forth in claim 15 are consistent with the understanding of a POSITA with experience in distributed computing.

84. Claim 15 then proceeds to recite “virtual objects” as follows: “normalizing the plurality of signals from each proprietary format to an Extensible Markup Language (XML) format to produce normalized signal data, wherein the XML format is configured to describe system policies through the use of virtual objects that comprise components of executable rules, and represents relationships between the virtual objects and corresponding devices, objects and

processes.” Claim 16 further recites “wherein the rule is constructed using a graphical visual policy editor that processes virtual objects, and wherein the physical security states and their relationships with network resources are managed and depicted as the virtual objects.”

85. The specification discusses various types of “objects” that a POSITA would understand to be object oriented programming components within a computer system. *See, e.g.*, ’088, 12:20-13:42 (discussing “building-block objects,” “visual rule objects,” “live objects,” “data objects,” “event objects”). The Jones Declaration in paragraph 128 similarly points to various object types in the specification, such as describing a number of object types, such as “HTML objects,” “data objects,” “embeddable software objects,” and “stencil objects.” *See, e.g.*, ’088, 6:51-54, 8:29-33, 19:53-46, 20:5-7, 20:37-38, 23:37-44.

86. These descriptions are generally consistent with the customary meaning of “object” in computer science in the relevant context. In this context, an “object” typically refers to a variable or data structure that contains information (which may include data and/or code in the context of object oriented programming) and/or represents something else.

87. The problem is that the “objects” described in the specification would already be considered “virtual” items in the sense that they are implemented by a computer system. I agree with the Jones Declaration in that regard regarding the “objects” described in the specification: “[e]ach of these objects are ‘virtual’ in the sense that they are implemented by a computer system.” Jones Declaration, ¶ 128. The problem, however, is that the claims do not merely recite “objects,” which would fit with the specification’s descriptions. Rather, the claims recite both “objects” and also “virtual objects,” which begs the question as to how “virtual objects” differ from other “objects” that are not virtual objects. The claim language and specification fail to answer that question with reasonable certainty.

88. As the Jones Declaration further notes regarding the “objects” described in the specification, “not all are ‘visual descriptions.’” *Id.* I agree with this point. Not all of the “objects” described in the specification are necessarily visual depictions. As the Jones Declaration further notes in paragraphs 129-130, dependent claim 16 further specifies functionality that “‘depict[s]’ the virtual objects visually.” I agree with the Jones Declaration where it asserts in paragraph 130 that a construction that defines “virtual objects” as something displayed visually “improperly incorporates these same concepts into claim 15 where they are not present.” Thus, it would not be understood by a POSITA that the defining characteristic of a “virtual object” is to be displayed visually. In other words, merely being displayed visually is not what makes an “object” into a “virtual object.”

89. The specification fails to provide guidance on the distinction between “virtual objects” and objects that are not virtual. The term “virtual objects” appears only in the claims. No mention of that term is provided in the specification. The only use of the word “virtual” is in an irrelevant mention of “VPN (Virtual Private Networking)” as an example of an application protocol for communication. ’088, 7:37-44.

90. Because the customary meaning of the term “object” in this context already entails that an object is created by a computer, i.e., virtual, a POSITA would be confused as to the meaning of “virtual object” as recited in the claims. The claim language would indicate, redundantly and confusingly, a “virtual virtual” variable or data structure in this sense. The patent fails to provide meaningful guidance as to what distinguishes an “object” from a “virtual object” in this context.

P. “reference” / “references” (’088, claim 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	Indefinite

	<i>Alternatively:</i> a shape used to create references for lookups for information
--	---

91. In my opinion, the term “references” in claim of the ’088 patent does not provide reasonable certainty as to the claim scope.

92. The claim language recites “defining a second plurality of objects representing actions, conditions and references” in claim 15.

93. It would not have been clear to a POSITA from the claim language or specification what “objects representing . . . references” means in this context.

94. The Jones Declaration in paragraph 132 points to two sections in the ’088 specification regarding “references,” but in my opinion these passages only demonstrate that the patent fails to provide reasonable certainty on the boundaries and claim scope. First, the specification states that “references” are a type of shape: “A number of basic types of shapes are utilized by the system: object shapes, condition shapes, actions shapes, modification shapes, references, and connectors.” ’088, 21:7-10 (underlining added). In the second section cited, however, the specification also mentions “references for lookups and comparisons”: “Reference shapes are used to create references for lookups and comparisons by the rules engine in real-time while processing the incoming data based on the preceding conditions.” *Id.*, 21:34-40 (underlining added).

95. In these descriptions of “references,” the ’088 patent uses the term “references” in two inconsistent and circular ways – as a shape, and as something that a shape is used to create. These passages render unclear the meaning of the term “references.” Are they shapes, as the specification first indicates, or are they items that shapes are used to create? And if “references” are items that a shape is used to create, what exactly are they then? The specification does not

provide sufficient further guidance. Where the specification states that “[r]eference shapes are used to create references for lookups and comparisons,” it is not reasonably clear what are the “references” for “lookups and comparisons” in this context. The mention that reference shapes are somehow “used to create references” does not provide meaningful guidance to a POSITA by elaborating on what that might mean.

96. The specification and claims thus fail to provide meaningful guidance as to what does and does not constitute “references” as recited in the claims. The specification thus would not give a POSITA reasonable certainty as to the scope of the term “references,” rendering the claim language indefinite in my opinion.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code.

Dated: November 17, 2022

By:



Stephen Gray