



February 23, 2024

Via Email

Christian E. Mammen
Womble Bond Dickinson (US) LLP
50 California Street, Suite 2750
San Francisco, California 94111
Chris.Mammen@wbd-us.com

Orrick, Herrington & Sutcliffe LLP
51 West 52nd Street
New York, NY 10019-6142
+1 212 506 5000
orrick.com

Richard F. Martinelli

E rmartinelli@orrick.com
D +1 212 506 3702
F +1 212 506 5151

Re: ***Arkose Labs Holdings, Inc. vs. DataDome, et al.,
Case No. 1:23-cv-01467-UNA (D. Del.)***

Counsel,

We write to put you on notice that the claims alleged by Arkose Labs Holdings, Inc. ("Arkose") against DataDome in the above-referenced action are totally without merit and, indeed, are frivolous. As set forth in detail below, it is clear that no reasonable pre-suit investigation was performed by Arkose and Arkose had no good faith basis to bring this suit. Rather, Arkose is obstinately continuing to inundate DataDome with a series of patents that have nothing to do with DataDome's technologies. For these same reasons, DataDome declines Arkose's offer to waive service here. Frankly, this complaint should never have been filed and should be immediately withdrawn. Should Arkose not dismiss these claims, DataDome will seek its fees pursuant to, at least, 35 U.S.C. § 285 and FRCP Rule 11.

U.S. Patent No. 7,373,510 ("the '510 patent") and U.S. Patent No. 9,148,427 ("the '427 patent") Are Invalid and Arkose's Infringement Allegations for Them Are Frivolous

1) The '510 and '427 Patents are Invalid Due to Obviousness-Type Double Patenting Over at Least Expired Related U.S. Patent No. 9,558,340 (the '340 patent')

The '510 and '427 patents are invalid for obviousness-type double patenting in view of the expired '340 patent. The '340 patent, '427 patent and '510 patent are part of the same family and all claim priority to the same application.

Although the '340 patent issued after the '510 and the '427 patents, it was the first in the family to expire. The claims of the '510 and '427 patents are not patentably distinct from the claims of the expired '340 patent, and are, therefore, invalid due to obviousness-

Christian E. Mammen
February 23, 2024
Page 2

type double patenting. *See Gilead Scis., Inc. v. Natco Pharma Ltd.*, 753 F.3d 1208,1216 (Fed. Cir. 2014).

Obviousness-type double patenting “is intended to prevent a patentee from obtaining a time-wise extension of patent for the same invention or an obvious modification thereof and prevents an inventor from claiming a second patent for claims that are not patentably distinct from the claims of a first patent.” *In re: Cellect, LLC*, 81 F.4th 1216, 1226 (Fed. Cir. 2023). The Federal Circuit has recently confirmed that obviousness-type double patenting applies here, where a later-issued related patent without patent term adjustment (“PTA”) expires before earlier-issued patents with PTA. *See id.*

Aside from being drawn to a method and computer program, as opposed to a system, the independent claims of the ’427 patent are essentially identical to those of the expired ’340 patent. The same is true of the corresponding dependent claims of each independent claim. The patentee plainly understood these claims were not patentably distinct from each other because in response to a double-patenting rejection during prosecution of the ’340 patent, it submitted a terminal disclaimer in view of the ’427 patent’s identical claims. *See* Ex. A (August 31, 2016 Amendment and Request for Reconsideration) at 7. The fact that the identical claims of the ’427 patent have not yet expired simply because the ’427 patent received a PTA extension, without a corresponding terminal disclaimer filed in the other direction, confirms that the ’427 patent claims are invalid. *See, e.g., Cellect*, 81 F.4th 1216.

The ’510 patent is no more than an obvious variation of the expired ’340 patent claims. Claim 1 of the ’510 patent is an obvious variation of the timer embodiment of claim 9 of the ’340 patent and is also an obvious variation of the process for stopping further requests in claims 6 and 7 of the ’340 patent. For example, there is no substantive difference between the verbs “checking” versus “determining”. *See Georgia-Pacific Corp. v. U.S. Gypsum Co.*, 195 F.3d 1322, 1327 (Fed. Cir. 1999)(finding claim of non-expired patent “merely an obvious variation of claim 1 of the [expired patent]” because the “minor linguistic difference does not serve to distinguish claim 1 of the [non-expired patent] from claim 1 of the [expired patent] in a nonobvious way”). Moreover, while claim 1 of ’510 patent includes some additional steps, these steps are the most obvious responses to the acts recited in claim 9 of the ’340 patent. For example, claim 9 of the ’340 patent does not expressly state that the request is not processed when the challenge is failed. But that is the natural thing to do.

A reasonable pre-suit investigation would have revealed that the claims of these patents are not patentably distinct from those of the expired ’340 patent and that these patents

Christian E. Mammen
February 23, 2024
Page 3

are invalid for obviousness type double-patenting. To the extent you were not aware of this fact, or the case law cited above, you are now. Your continued maintenance of this suit would be a violation of Rule 11 and exceptional.

2) Arkose's Infringement Allegations for the '510 and '427 Patents are Frivolous

Putting aside the clear invalidity of the '510 and '427 patents, Arkose has substituted two related patents for one that DataDome has already explained that it plainly does not infringe. In the parties' prior correspondence, Arkose accused DataDome's puzzle slider CAPTCHA of infringing claim 1 of the now-expired, related '340 patent discussed above. We refer you to my December 1, 2023 letter, which explained that "there is no possible reasonable infringement allegation" against DataDome for claim 1 of the '340 patent. Ex. B (12/1/2023 Letter from R. Martinelli to C. Mammen). Unsurprisingly, Arkose decided to not bring suit on the '340 patent. However, Arkose now accuses the *same* puzzle slider of infringing the *exact* same claim language, without support that could show plausible infringement of claim 1 of the '427 patent.

In addition to the reasoning in my prior letter, Arkose should have been fully aware that DataDome does not infringe either the '427 patent or the '510 patent because both are directed to a method of preventing robots from browsing a Web site when an "*initial* request" is received from an "*undefined originator*," *i.e.*, a user has not been judged to be a human or a robot. If a challenge presented to the undefined originator is successfully fulfilled, they are assumed to be a human being and the site processes their initial request and all subsequent ones. '427 patent, 2:46-52. If the challenge is not successfully fulfilled, the undefined originator is assumed to be a robot and no further requests are processed. *Id.* In short, any new and "undefined" entry prompts a challenge to verify whether the user is a human or a robot. The purpose of this invention is to prevent website access by robots "without requiring end users to register or the site administrator to have to manage an access list of authorized users." *Id.* at 2:58-61.

However, DataDome's service does not possess the concept of an "undefined originator" that is then judged to be a human or not. Indeed, DataDome recognizes that sometimes unauthorized users include a combination of human and bot traffic. And DataDome does not issue a CAPTCHA in response to an initial request. Rather, CAPTCHAs are used *after* a user has interacted with and provided requests to the subject website that allow DataDome to define the user as suspect.

Christian E. Mammen
February 23, 2024
Page 4

Arkose's allegations are particularly unreasonable because both the '427 and '510 claim charts affirmatively demonstrate that DataDome's accused CAPTCHA functionality does not perform the asserted claims because DataDome's CAPTCHA is not triggered in response to an "initial request" from an "undefined originator." Rather, the accused DataDome CAPTCHA functionality is only performed in response to expressly defined originators. Arkose's charts show the user definitions that potentially lead to the use of a CAPTCHA, e.g., when a user is browsing and clicking at a speed much faster than expected of a human, when Javascript is prevented from working, and when there is a robot on the same network (IP) as the user. See Compl. Ex. G, H at [1a]. DataDome's CAPTCHA is thus used in the specific situations above where the originator is defined in such a way that verification is required.

Beyond these overarching reasons why the accused DataDome functionality cannot infringe the '427 and '510 patents, it is also not infringing for at least the following additional reasons specific to each of the asserted claims.

'427 Patent Claim 1

The '427 patent claims require that the claimed challenge must include "a plurality of graphical forms, and an accompanying textual expression describing one of the plurality of graphical forms," wherein "the response to the challenge includes an identification of a location of the described one of the plurality of graphical forms." For example, Figures 5-a and 5-b show that such a challenge is one that contains multiple images and requires the user to identify a single image from this grouping as the correct image in response to the accompanying text.

DataDome has already explained to Arkose why this is not infringing with respect to Arkose's previous, analogous claim chart for the identical claims of the related '340 patent. See, e.g., Ex. B (12/1/2023 Letter from R. Martinelli to C. Mammen). Here again, Arkose's '427 patent claim chart accuses DataDome's puzzle slider, where the user completes a CAPTCHA by sliding the missing puzzle piece to fill the puzzle. DataDome's CAPTCHA does not resemble Figures 5-a and 5-b in the slightest, and also has no relationship to the '427 patent claims. The accused CAPTCHA does not have a "plurality of graphical forms" because the CAPTCHA only has a single puzzle piece. DataDome's CAPTCHA also does not require the user to **identify** the location of any of the plurality of graphical forms. Instead, the CAPTCHA itself identifies the location of the missing puzzle space for the user, and the user slides the piece to complete the puzzle. There is no identification from a plurality of graphical forms through sliding a missing puzzle piece to its predetermined designated space.

Christian E. Mammen
February 23, 2024
Page 5

Troublingly, Arkose appears to be attempting to recapture the prior art that it told the patent office was **not** covered by the claims during prosecution — a challenge involving a location that the system instructs the user to interact with — which the patentee expressly distinguished from the requirement in the claims that the user identify one of many possible graphics. In the 3/15/2012 Appeal Brief in the '427 patent file history, the applicant distinguished the Blonder prior art reference as follows:

Blonder teaches a graphical password arrangement that displays a predetermined graphical image and **requires a user to “touch” predetermined areas of the image** in a predetermined sequence, as a means of entering a password. **It is not clear how this teaches a challenge that includes a plurality of graphical forms and an accompanying textual expression describing one of the plurality of graphical forms, as recited in claim 56.** First, it is noted that in Blonder there is only one graphical image, not a plurality of graphical forms. Second, in Blonder the user is prompted to touch predetermined areas of the image in a predetermined sequence. Therefore, in Blonder **the prompt instructs what the user is required to do, but does not describe one of the plurality of graphical forms.**

See Ex. C (3/15/2012 Appeal Brief) at 10-11 (emphasis added).

The Applicant further emphasized that “an important feature of the [] invention is...the accompanying textual expression **provides the answer to the challenge** and a human being after reading the textual expression should be able to select the correct graphical form.” *Id.*

In contrast to this, DataDome’s puzzle slider’s only textual expression is “[s]lide right to fill the puzzle” which is merely a text prompt that “instructs what the user is required to do, but does not describe one of the plurality of graphical forms.” In allowing the '427 patent, the Board found this type of text prompt is **not** a “textual expression within the meaning of claim 1.” Rather, in the 3/3/2015 Patent Board Decision, the Board found that “[a] prompt [that] instructs a user to select a [] region and position it within the password region” does not “teach or suggest an accompanying textual expression describing the graphical form.” Ex. D (3/3/2015 Patent Board Decision) at 7-8.

A reasonable pre-suit investigation would have included a review of the '427 patent’s file history and a recognition that your infringement theory directly contradicts the

Christian E. Mammen
February 23, 2024
Page 6

arguments made to the patent office to secure allowance of the subject claims. To the extent you were not aware of this aspect of the file history, you are now. Your continued maintenance of this suit in view of this is a violation of Rule 11 and exceptional.

'510 Patent Claim 1

Arkose's infringement chart for the '510 patent similarly contains a number of additional deficiencies beyond the general ones discussed above. Claim 1 of the '510 patent requires that, in response to a failed attempt by a robot to access a website, a "timer [is] started so that access to the site may be temporarily barred, from that IP source address." See '510 patent cl. 1, 4:10-15. The claim chart fails to show that DataDome's CAPTCHA starts a timer in response to a failed challenge from an undefined originator, as claimed.

Arkose accuses DataDome's "timeboxing" and "rate limiting" features, but neither has anything to do with an undefined originator's failed attempt to access a website. The "timeboxing" feature sets a rule that allows the web server "to select a time period (specific hours on specific days of the week) during which the traffic should be allowed" and select a "CAPTCHA or block response for the remaining traffic" outside of the time period. See, e.g., Compl. Ex. G at 1[d]. The "rate limiting" feature allows the web server "to define a volume threshold (by providing the value of the number of requests during a time period of either one hour or one day) below which the traffic should be allowed" and then set a "CAPTCHA or block response for the traffic that exceeds the volume threshold." *Id.* The "timeboxing" and "rate limiting" features set **when** a CAPTCHA is enabled, and not a "timer" that tracks the length of time an IP address is barred from accessing the website in response to failing a CAPTCHA.

Since Arkose can point to no evidence that DataDome's CAPTCHA employs the claimed timer, Arkose's allegations and pre-suit investigation are improper. Arkose's infringement allegations for any of the claim limitations that relate to timer expiration (*i.e.*, "checking whether said timer has expired" and "dropping or redirecting said TCP connection" based on the expired timer) fail.

DataDome's CAPTCHA also does not log and use a "source IP address" in response to a failed CAPTCHA. There is no indication that a "logged IP address" is reset in response to an expired timer or that the source IP address is compared with the "logged source IP address" in determining whether a new request is allowed to proceed normally. See, e.g., '510 patent cl. 1. Arkose's infringement allegations cite to a

Christian E. Mammen
February 23, 2024
Page 7

“SkipIPs” feature but there is no indication that it is set in response to a user failing a CAPTCHA, nor does it indicate whether the “source IP address” is logged or that the IP address is reset in response to an expired timer. This is because DataDome’s CAPTCHA does not use “a source IP address” in any further steps after the user fails a CAPTCHA challenge.

DataDome explained to Arkose that “there is no possible reasonable infringement allegation” for claim 1 of the related ‘340 patent prior to this suit. See Ex. B (12/1/2023 Letter from R. Martinelli to C. Mammen). Arkose’s infringement allegations for the ‘427 and ‘510 patents are similarly deficient. Arkose’s dogged pursuit of infringement claims for related patents that fail for many of the same reasons demonstrate that Arkose did not perform a reasonable pre-suit investigation and is asserting these patents merely to harass DataDome.

U.S. Patent No. 10,082,954 (“the ‘954 patent”) and U.S. Patent No. 10,599,330 (“the ‘330 patent”) Are Invalid and Arkose’s Infringement Allegations for Them Are Frivolous

1) The Claims of the ‘954 and ‘330 Patents Recite Abstract Ideas and Are Invalid Under 35 U.S.C. § 101

The ‘954 and ‘330 patents each claim abstract mental processes and/or mathematical concepts in violation of 35 U.S.C. § 101.¹ In particular, the claims of the ‘954 and ‘330 patents recite a series of steps for authenticating a user by measuring the characteristics of actions they perform. And, instead of specifying how, technologically, those abstract ideas are implemented, the claims simply list steps describing general, conceptual ways to measure and assess this data using functional, results-oriented language, applying only a generic computer environment. Such “vague, functional” terms, “devoid of technical explanation as to how to implement the invention,” are abstract. *TLI Communs. LLC v. AV Auto., L.L.C.*, 823 F.3d 607, 615 (Fed. Cir. 2016); see also *Two-Way Media v. Comcast*, 874 F.3d 1329, 1337 (Fed. Cir. 2017) (finding claims directed to routing information abstract because they “[did] not sufficiently describe how to achieve these results in a non-abstract way”).

The common specification of the ‘954 and ‘330 patents explains that the problem they seek to address relates to the common and well-understood “need to ensure that a user

¹ DataDome believes that the claims of the other asserted patents are also invalid under § 101 as well (see a discussion of why for the ‘049 and ‘232 patents below) and reserves all rights to more fully argue so in the future.

Christian E. Mammen
February 23, 2024
Page 8

of a computing device is the owner of the computing device or is otherwise authorized to use the computing device.” ’954 patent at 1:8-10. The specification criticizes prior art solutions for potentially allowing “phishing,” wherein “an individual [] in possession of stolen credentials” uses “the stolen credentials to successfully pose as the authorized user when using the computing device.” *Id.* at 1:14-19.

The allegedly inventive solution to this problem is nothing more than the common, and old, practice of identifying a unique characteristic of a user and then using that characteristic to confirm their identity. This concept is phrased in the generic, functional claim language of first “measuring one or more characteristics of a user action” at a time when they have already been authorized, “recording the user action and the measurements of the characteristics” that “meet a uniqueness condition” differentiating them from other users, and then later authenticating a user as that same user by again measuring their characteristics and “determining that the measurements of the characteristics of the prompted actions performed by the current user meet a similarity condition with respect to [the previously recorded] measurements.” *Id.* at 1:23-47.

The concepts disclosed and claimed are mere generic computerizations of age-old authentication techniques. Indeed, the humble signature is a user action whose uniqueness is recognized and used to authenticate the person who made the signature. Critically, the patents do not claim any “particular way of programming or designing the software” or disclose “how this would be technologically implemented.” *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241, 1244 (Fed. Cir. 2016).

Moreover, there are no unconventional technological details in the patents’ specification. The patent admits that its disclosed method is done using nothing more than a general purpose computer: “These computer readable program instructions may be provided to a processor of a general purpose computer.” ’954 patent at 3:22-23. But when claims recite conceptual, mental steps of the type that can be performed by a human mentally or using a pencil and paper, and merely requires their implementation on a computer, they are invalid. *See, e.g., PersonalWeb Techs. LLC v. Google LLC*, 8 F.4th 1310, 1316 (Fed. Cir. 2021) (“mental processes that ‘can be performed in the human mind’ or ‘using a pencil and paper’ are “a telltale sign of abstraction”) (citing *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1371–72 (Fed. Cir. 2011) and *Parker v. Flook*, 437 U.S. 584, 586 (1978)).

Further emphasizing the lack of a technical implementation, the patent expressly notes that the user measurements are taken using any “known type of user input that may be sensed by computing device 100 in accordance with **conventional techniques**.” ’954

Christian E. Mammen
February 23, 2024
Page 9

patent at 4:16-19 (emphasis added). And the specification further makes clear that uniqueness evaluations that are performed on the measured data are nothing more than well-known, abstract mathematical calculations, such as the “Fisher combined probability test” and the “Friedman test.” See *id.* at 7:19-8:3. Moreover, the claims are not even limited to these conventional tests.

The ’954 and ’330 patents themselves thus make clear that the claimed invention is nothing more than the implementation of mental steps on a general purpose computer. This understanding is indeed recited in the claims themselves, which claim a series of generalized pencil and paper steps, and then a general purpose computer at the end as an afterthought. See, e.g., ’330 patent claim 1:

1. A method, for challenging a user of a computing device, the method comprising:

[mentally-performable “measuring,” “determining,” “recording,”
“performing,” “selecting,” and “prompting” steps]

wherein the measuring, determining, recording, performing, selecting, and prompting are implemented in any of

- (a) computer hardware, and
- (b) computer software embodied in a non-transitory, computer-readable medium.

’954 patent claim 1 claims the same functionality in the same manner, in the form of a “system for challenging a user of a computing device.”

These claims fail both prongs of the test set forth in *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 223 (2014).

First, because the claims recite nothing more than a series of steps for gathering data, evaluating that data, and authenticating a user based on that evaluation, as implemented on a general purpose computer, they are directed to nothing more than abstract ideas and fail *Alice* step one.

The Federal Circuit has repeatedly found that claims such as these are merely directed to abstract ideas.

Christian E. Mammen
February 23, 2024
Page 10

For example, *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1352 (Fed. Cir. 2021) invalidated a number of similar claims, including those “directed to the abstract idea of collecting and examining data to enable authentication.” The same was the case for claims in other USR patents that both collected a first set of biometric information, and then later used it to authenticate that user alongside additional a “second authentication information.” *Id.* at 1354 (claims are invalid when they “generically provide for the collection of biometric information to generate a first authentication information, and then authenticating a user using both the biometric-information-derived first authentication and a second authentication information.”).

As another example, *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) invalidated claims to “(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources” as directed to the abstract idea of “providing restricted access to resources.”

Similarly, the *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093–94 (Fed. Cir. 2016) opinion invalidated a method that “collects information regarding accesses of a patient's personal health information, analyzes the information according to one of several rules (i.e., related to accesses in excess of a specific volume, accesses during a pre-determined time interval, or accesses by a specific user) to determine if the activity indicates improper access, and provides notification if it determines that improper access has occurred.”

As is the case for the '954 and '330 patents, the Federal Circuit treats “analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, as essentially mental processes within the abstract-idea category.” *Id.*; see also *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (because the “realm of abstract ideas” includes “collecting information, including when limited to particular content,” claims with a focus “on collecting information, analyzing it, and displaying certain results of the collection and analysis” are invalid).

The Federal Circuit has also repeatedly rejected arguments that abstractness is avoided due to some tangential relationship to “providing increased [] security” or “a security protocol.” See *In re AuthWallet, LLC*, No. 2022-1842, 2023 WL 3330298, at *3 (Fed. Cir. May 10, 2023). A “security” feature would not render the claims non-abstract “for the same reason that the patents in Universal Secure Registry were found to speak to

abstract ideas.” *Id.* (citing *Universal Secure Registry*, 10 F.4th at 1354–55 (finding claims that “generically provide[d]” for the collection of information to perform authentication of a user in a manner that was “conventional” to be directed to an abstract idea)). Moreover, the claims here “do[] not speak to specific or technical problems and solutions but rather recite[] generic steps and results.” *Id.* In short, the addition of another abstract idea does not render the claims non-abstract. *Id.*

Because “the focus of the claims is not on [] an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools,” they are directed to nothing more than those abstract ideas. *Elec. Power Grp.*, 830 F.3d at 1354.

The claims of the ’954 and ’330 patent also fail *Alice* step two, because the elements of the claims, both considered as a whole and individually, do not recite an inventive concept that amounts to significantly more than the abstract idea itself.

This is because “[t]here is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique.” *Universal Secure Registry*, 10 F.4th at 1353. Beyond their generic data collection and evaluation steps, the claims recite nothing more than that what specification itself admits is the use of a general purpose computer. These components cannot do more than their well-understood, routine, and conventional activities because the patents do not teach anything more. Because the “claims in this case do not even require a new source or type of information, or new techniques for analyzing it,” they plainly do not even “require an arguably inventive set of components or methods, such as measurement devices or techniques, that would generate new data” and “do not invoke any assertedly inventive programming.” *Elec. Power Grp.*, 830 F.3d at 1355.

And the Federal Circuit has repeatedly held that the recitation of nothing more than “off-the-shelf, conventional computer [] technology for gathering, sending, and presenting the desired information” are **not even arguably inventive** and indisputably fail *Alice* step two. *Id.* (emphasis added).

2) Arkose’s Infringement Allegations for the ’954 and ’330 Patents are Frivolous

The accused technology is so vastly different than the ’954 and ’330 patents that Arkose’s infringement allegations are frivolous. Indeed, the accused technology is not

Christian E. Mammen

February 23, 2024

Page 12

even attempting to solve the same problem as the user authentication performed by the '954 and '330 patents.

The '954 and '330 patents relate to measuring the **unique** characteristics of actions performed by a **specific**, already-authorized user, and then later issuing a challenge to an unauthorized user attempting to access a sensitive resource that prompts them to perform another action to see if those unique characteristics are again present, which is said to securely identify them as the authorized user. See, e.g., '954 patent at 1:8-48.

For example, if a specific pre-authorized user draws a line connecting dots on a touch screen that has a specific individualized curvature, that curvature is considered unique and can serve as a basis for later authenticating that specific user. See *id.* at 7:9-18:

While doing this, the current user may be challenged to draw on a touch screen of the computing device a set of geometric features learned from the authorized user's typing history. For example, the curvature of the shape connecting a set of dots as part of a challenge must match the curvature of the same shape previously generated by the authorized user.

Other examples of uniqueness conditions the patents discuss include the volume of voice input, angle and speed of tactile input, and typing speed of keyboard input. See, e.g., *id.* at 4:36-45.

In stark contrast, DataDome's technology does not attempt to authenticate specific users and as such makes no user specific measurements and certainly no measure of user "uniqueness." The allegations in the Complaint do not allege otherwise.

Arkose's claim charts assert nothing more than that "behavioral data" "such as mouse movements or key strokes" can be collected. See, e.g., Compl. Ex. I at p. 5. But there is no evidence any of that information is unique or user specific. Indeed, the evidence cited elsewhere in the claim charts expressly shows that the collected data is for **all users** without any individualization. See *id.* at p. 7. Even if, in certain limited occasions, the DataDome system may issue a CAPTCHA challenge upon detecting suspicious activity, there is no suggestion that this challenge involves recording or attempting to identify any unique measurements for that specific user, much less comparing new measurements with existing pre-authenticated measurements for that same user. See *id.* at p. 11.

Christian E. Mammen
February 23, 2024
Page 13

In view of this, it is unsurprising that the evidence Arkose has charted not only fails to show that the claims are met – it affirmatively shows that DataDome does not practice the asserted claims.

For example, there is no basis to assert that DataDome could meet most of charted '954 patent claim 1 for at least the following reasons.²

DataDome does not have a “characteristics measurement module configured to measure one or more characteristics of **a user action** sensed by a computing device and performed **by an authorized user** of the computing device **subsequent to the authorized user of the computing device having been identified as the authorized user** of the computing device” as recited in '954 patent claim 1. Arkose points to no evidence that DataDome does anything like this because it does not. DataDome doesn't measure characteristics of a particular “authorized user.” There is no attempt to track particular users and deem them authorized or unauthorized.

Because DataDome is not trying to identify and authenticate individual users, it also does not have “a uniqueness assessor,” which is required throughout the '954 patent claim 1 limitations that relate to it. The accused technology does not measure specific user actions to determine the uniqueness of those actions.

DataDome does not have “a challenge manager” for “determining that the measurements of the characteristics of the selected challenge actions performed by the current user meet a similarity condition with respect to measurements of corresponding characteristics of the selected challenge actions” as recited in '954 patent claim 1. The accused technology does not compare measured actions by specific users to compare them with past actions performed by that same user.

As with the '510 patent, it is troubling that Arkose is again ignoring the prosecution history of its own patents, which demonstrate that there can be no infringement. For example, in the 3/22/2018 Amendment in the '954 patent's file history, the applicant argued that:

² '330 patent claim 1 is substantially similar to '954 patent claim 1 and accordingly Arkose's infringement allegation for it suffers from all of the same flaws.

Christian E. Mammen
February 23, 2024
Page 14

The claimed invention, with regard to [the “determine” and “cause” limitations for the “uniqueness assessor”], thus 1) measures an action that is known to have been **performed by an authorized user** of a computing device, 2) determines that the measurement meets a uniqueness condition relative to a comparison set that includes measurements of corresponding actions, and 3) **records the authorized user’s action** and its measurement **only if its measurement meets the uniqueness condition**.

Ex. E (3/22/2018 Amendment) at p. 6; see *also* Ex. F (10/8/2017 Amendment) at p. 7. Arkose makes no attempt to show that these specific features – that were highlighted to argue for the patentability of the claimed invention – appear in the accused product. Of course, they do not.

The fact is that Arkose could not have undertaken an adequate and reasonable pre-suit investigation because it apparently does not understand the basic functionality of DataDome’s product.

U.S. Patent No. 10,147,049 (“the ’049 patent”) and U.S. Patent No. 11,227,232 (“the ’232 patent”) Are Invalid and Arkose’s Infringement Allegations for Them Are Frivolous

1) The Claims of the ’049 and ’232 Patents Recite Abstract Ideas and Are Invalid Under 35 U.S.C. § 101

The ’049 and ’232 patents each claim abstract mathematical concepts in violation of 35 U.S.C. § 101.³ In particular, the claims of the ’049 and ’232 patents recite a series of steps for gathering and manipulating data for generating a statistical model about a target user’s behavior. And, instead of specifying how, technologically, those abstract ideas are implemented, the claims simply list the required data manipulation steps using functional, results-oriented language and applies only a generic computer environment.

The claims of these patents are directed to no more than data gathering and manipulation—in particular, to accessing data samples for a plurality of users and generating a normal sample data set and an abnormal sample data set using such data. For example, claim 1 of the ’049 recites:

³ As noted above, DataDome believes that the claims of the other asserted patents are also invalid under § 101 as well (see a discussion of why for the ’954 and ’330 patents above) and reserves all rights to more fully argue so in the future.

Christian E. Mammen
February 23, 2024
Page 15

1. A method, comprising:

[a] for a system or application used by a plurality of users, **providing** an access to a memory device storing user data samples for all users of the plurality of users;

[b] **selecting** a target user from among the plurality of users; and

[c] using a processor on a computer and using data samples for the target user and data samples for other users of the plurality of users, **generating** a normal sample data set and an abnormal (anomalous) sample data set to serve as a training data set for training a model for an anomaly detection monitor for the target user such that the data samples of the target user are used to derive a normal sample data set for the training set and the data samples of other users are used to derive an abnormal sample data set for the training set.

'049 patent at 18:14-29 (emphasis added). As emphasized, the claim is directed to a series of functional steps that call for either: (1) data gathering (providing an access to a memory device storing user data samples or selecting a target user) or (2) data manipulation (generating a normal sample data set and an abnormal sample data set using the gathered data). The '232 patent recites similarly generic limitations of “providing an access to a memory device” and “selecting a target user.” While the '232 claims recite an additional data gathering step of “tak[ing] data samples for the target user to generate a normal sample” and a mathematical formula of “using a local outlier factor (LOF) function to generate an abnormal sample data set,” these limitations add nothing more than further abstract mathematical concepts.

These claims fail both prongs of the test set forth in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 223 (2014).

First, because the claims recite a series of steps for gathering, manipulating, and displaying data, they fail the first step of the *Alice* analysis. Each of the steps is a form of data collection or manipulation. Steps [a] and [b] above are each data collection: providing access to a memory device storing user data samples and selecting a target user from all user data samples. Step [c] recites data manipulation: using a generic “processor” to generate a normal sample data set and an abnormal (anomalous) sample data set to serve as a training data set for training a model. Indeed, step [c]

Christian E. Mammen
February 23, 2024
Page 16

recites nothing more than basic math and statistics: generating data models and determining normal samples versus outliers.

The Federal Circuit has consistently recognized that claims directed to data gathering, manipulation, and organization are “a familiar class of claims ‘directed to’ a patent-ineligible concept.” *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1352-54 (Fed. Cir. 2016) (finding claims reciting a method of detecting events on an interconnected electric power grid being directed to abstract ideas of collecting information, analyzing it, and displaying certain results).

Citing the same authority, the District of Delaware has similarly found claims directed to conventional machine learning techniques described in broad functional terms, as here, to be ineligible under the first prong of *Alice*. *Recentive Analytics, Inc. v. Fox Corp.*, No. CV 22-1545-GBW, 2023 WL 6122495 (D. Del. Sept. 19, 2023). In *Recentive Analytics*, this Court invalidated a family of “Machine Learning Training Patents” that were directed to a computer-implemented method of generating an event schedule through a machine learning model that has been iteratively trained to optimize target features (e.g., attendance, profit, revenue, expenses) based on input parameters. *Id.* In doing so, the Court rejected essentially every possible argument that Arkose might make in defense of these patents: 1) that “machine learning algorithms process information differently from the human brain,” because machine learning is algorithmic in nature, and so the patents are directed to an abstract idea; 2) that “the claimed processes require too much data and computing power for the human brain to do,” because the patents merely use a computer as a tool; and 3) that limited caselaw involving claiming “specific and unconventional” rules involving “changing a subjective process where artists are trying to make a piece of art look good” has no applicability to this machine learning context, which does not involve “practical, technological improvements extending beyond improving the accuracy of a mathematically calculated statistical prediction.” See *id.* at *8-11.

Delaware is not alone in this regard. For example, even the Western District of Texas has invalidated claims to a “machine-learning method of generating datasets” at the motion to dismiss stage for similar reasons. See *Health Discovery Corp. v. Intel Corp.*, 577 F. Supp. 3d 570 (W.D. Tex. 2021).

Second, these claims are abstract because they do not recite any technology for performing the recited steps. The lack of specificity in these claims also means the steps can be performed entirely in the human mind. For example, a computer programmer or statistician could observe data samples for all users, select a target user

Christian E. Mammen

February 23, 2024

Page 17

from these data samples, and generate a normal and abnormal sample data set. Similarly, the human could also perform a local outlier function in the mind to generate the abnormal sample data. There is no requirement in these claims that the generation of the normal and abnormal data sets be through any particular method of technique aside from the use of a general-purpose processor. In other words, the elements of the claims, both considered as a whole and individually, do not recite an inventive concept that amounts to significantly more than the abstract idea itself.

As with the '954 and '330 claims, the subject claims recite nothing more than what the specification admits is the use of a general-purpose computer to perform generic data collection and evaluation steps. For example, the '049 patent expressly states that the "computer system/server 1012 ... is shown in the form of a **general-purpose computing device**" and that the invention is not even limited to this as "embodiments of **the present invention** are capable of being implemented in conjunction with **any other types of computing environment now known or later developed**." '049 patent at 15:45-47, 13:45-51 (emphasis added). And as described in the specification, these components cannot do more than their well-understood, routine, and conventional activities because the patents do not teach anything more. There is no limitation on how the data is being used to train a model or any unconventional hardware needed to train a model to even arguably improve the underlying computing device. In other words, the claims simply do not limit **how** "normal sample data" and "abnormal sample data" is "generated" as claimed. This is because the normal sample data and abnormal sample data already exist – the claims merely require labeling existing data samples as such. Indeed, the claims in this case do not require an arguably inventive set of components or methods, such as measurement devices or techniques, that would generate new data. *Elec. Power Grp.*, 830 F.3d at 1355. The claim elements here are purely functional and generically require data sets for other users to be excluded from the normal sample data for the specific user.

Where the claims are directed to an abstract idea under prong one of *Alice*, the claims do not survive *Alice* prong two where the claims only recite generic and conventional hardware – a processor on a computer or a memory device. This is precisely the case here, as the claimed generic computer components do nothing more than well-understood, routine, and conventional activities previously known to the industry.

2) Arkose's Infringement Allegations for the '049 and '232 Patents are Frivolous

As with Arkose's other allegations, the accused technology is completely different than what is discussed in these patents. Once again, these patents are directed to

Christian E. Mammen
February 23, 2024
Page 18

authentication of a specific individual user. To accomplish this, the '049 and the '232 patents disclose methods for anomaly detection using machine learning techniques. The common specification of these patents frames the purported invention by explaining that prior art solutions generate artificial samples for training that do not reflect real cases and assume an underlying data distribution, which it says is unrealistic in multi-user environments. See, e.g., '049 patent at 2:35-45.

To address these alleged problems with the prior art, the patents disclose using a method to train a machine learning model by generating both benign and malicious training samples from unlabeled data to filter out bad normal samples and generate potential anomalous samples **for each target user**. *Id.* at 2:48-55.

A key intuitive concept underlying **the present invention** is that, when there are many users, other users' behavior can provide additional insights on potential anomalies. Thus, it is assumed that **a user's actions are similar to each other**.... However, when data samples from many users are combined, they provide more accurate projection of the entire data space and help to estimate accurate **boundaries between different users**. Thus, a key feature of the present invention is to provide a mechanism to generate anomalous samples automatically from other users' behaviors where all samples of all users in the data set (including benign samples from the target user's own data points) are examined, and samples that are considered different from a target user's data samples are identified.

Id. at 4:63-5:15. As can be seen, the "present invention" is described as relying on "other users" to identify anomalies. The target user's normal behavior is learned using training samples of the target user's own past behavior samples, whereas the target user's possible abnormal behavioral patterns, e.g., what makes the user unique and therefore authenticatable, can be learned from other users' training samples, since the other users expectedly exhibit quite different behavioral patterns from the target user. *Id.* at 4:15-27. The patents refer to the estimation of the degree of "outlier-ness" with respect to samples of a target user and to select anomalous samples for the target user from other users' data samples as an extension of the Local Outlier Factor (LOF). *Id.* at 5:15-20.

This alleged invention of training a model to recognize a specific target user described above is embodied in essentially every limitation of the independent claims. For example, '049 patent claim 1 recites that "the training data set training a model for an anomaly detection monitor **for the target user** [is] such that the data samples of the

Christian E. Mammen
February 23, 2024
Page 19

target user are used to derive a normal sample data set for the training set and the data samples **of other users** are used to derive an abnormal sample data set for the training set,” and ’232 patent claim 1 recites “using a local outlier factor (LOF) function to generate an abnormal sample data set for training the ***anomaly detection monitor for the target user.***”

Notably, during prosecution of the ’049 patent, applicant amended the claims to include the derivation of the training set and expressly argued the need for the invention to train the system for ***specific target users*** and distinguished prior art because “there is no description [in either cited prior art] of the derivation of a training set of data for the [target] user.” 6/26/2018 Amendment at p. 8. Applicant further explained:

[N]either [cited reference] is aware of the concept disclosed in the present invention for deriving a training data set for training a model for an anomaly detector monitor ***for each target user.*** In the claimed invention, this training set ***for each target user*** is derived by using ***the target user’s own data*** as normal sample data for the training set and the abnormal sample data for the training set of the anomaly detector for the target user is derived using sample data of other users.

Ex. G (6/26/2018 Amendment) at p. 9 (underline emphasis original). Applicant further notes that, as explained in the originally-filed specification, “the present inventors have recognized a problem in this art is obtaining training sample sets for training an anomaly detector monitor ***for specific users.***” *Id.*

Despite Applicant’s own emphasis on this alleged novelty, the DataDome technology accused in the Complaint has no relationship to deriving any training data set for training a model for an anomaly detector monitor ***for each target user*** by using the ***target user’s own data as normal sample data*** and using ***sample data of other users as abnormal sample data***, as required by the claims of the ’049 and ’232. Moreover, a training for individual target users makes no sense in the context of DataDome’s system, which must deal with multitudes of unknown users accessing public websites.

In fact, the charted material is so vague and unrelated to the technical problem or solution of the ’049 and ’232 patents that it is difficult to understand exactly what Arkose is accusing. Arkose’s claim charts assert nothing more than that the “AI Threats Detection” functionality collects signature-based, behavioral, reputational, or vulnerability scanner information. See, e.g., Compl. Ex. J at p. 21. The evidence cited

Christian E. Mammen
February 23, 2024
Page 20

further shows that “gesture” information can be collected. See *id.* at 23. But this evidence does not show any normal sample data based on a target user’s own data or sample data of other users as abnormal sample data.

Fatally, Arkose’s claim charts confirm that “[a]ll data collected by the SDK is completely anonymous and does not reveal the identify of the user.” See *id.* at p. 24. In other words, DataDome’s systems do not maintain separate user profile data for target users to be used as their own normal sample data. Similarly, DataDome’s systems do not derive abnormal sample data using local outlier factors, or any other algorithm. As before, in certain limited occasions, the DataDome system may issue a CAPTCHA challenge upon detecting suspicious activity. But there is no suggestion that this challenge is based on a machine learning training data set **for that specific user**, much less a training data set that is derived from a target user’s own data as normal sample data and using sample data of other users as abnormal sample data. Even more generally, there is nothing suggesting that the DataDome system “train[s] a model for an anomaly detection monitor for the target user” (*i.e.*, for a particular user).

To avoid any ambiguity, DataDome’s systems simply do not derive training data sets for training a model for an anomaly detector monitor for specific users by using a user’s own data as normal sample data for the training set and using sample data of other users as abnormal sample data for the training set. A reasonable pre-suit investigation would have confirmed this.

Arkose’s Advertising Claims Are a Meritless Attempt to Cover Up Its Own Misleading Comparative Advertising

Arkose’s complaint is equally deficient when it comes to its advertising claims. At the outset, we note that Arkose lacks standing to sue under the Federal Trade Commission Act (“FTCA”) and under California’s False Advertising Law (“FAL”). There is no private right of action under the FTCA for competitors or consumers; only the FTC can enforce 15 U.S.C. § 45(a). See *e.g. Li Xi v. Apple Inc.*, 603 F. Supp. 2d 464, 470 (E.D.N.Y. 2009). Arkose has no standing to sue under California’s False Advertising Law because Arkose does not and cannot allege it relied on DataDome’s comparative advertising. See *e.g., Clorox Co. v. Reckitt Benckiser Grp. PLC*, 398 F. Supp. 3d 623, 646 (N.D. Cal. 2019) (under FAL and unlawful prong of UCL, plaintiff must demonstrate it “suffered an injury due to his or her own actual and reasonable reliance on the purported misleading statements”); *In re Outlaw Lab’y, LLP*, 463 F. Supp. 3d 1068, 1086 (S.D. Cal. 2020) (same).

Christian E. Mammen
February 23, 2024
Page 21

Comparative advertising is expressly encouraged by the Federal Trade Commission because it allows businesses like DataDome to inform consumers about product alternatives. See, e.g., 16 C.F.R. § 14.15(c) (“Comparative advertising encourages product improvement and innovation, and can lead to lower prices in the marketplace.”). Indeed, as two renowned scholars have noted, the law provides “an affirmative right” to businesses, like DataDome, that use advertising to compare their products to alternatives. S.L. Dogan & M.A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 Hous. L. Rev. 777, 796 (2004).

Courts analyze advertising in its full context. *Freeman v. Time, Inc.*, 68 F.3d 285, 289–90 (9th Cir. 1995) (affirming dismissal because no reasonable consumer would be confused by advertiser’s disclosures). Most significantly here, the full context of DataDome’s comparative advertising—during the short few months it was available on DataDome’s website—shows DataDome disclosed the full details in its advertising, so the advertising is accurate, not false or misleading. For example, DataDome’s comparison linked directly to the G2 reviews, in which there multiple complaints about Arkose’s dashboard. No reasonable consumer would be confused or misled in the context of the comparison statement.

Arkose’s comparative advertising claims fail under the Lanham Act and the Delaware Deceptive Trade Practices Act for the additional reason that Arkose cannot and does not plausibly allege any injury resulting from the comparison page. Indeed, it can point to no lost business as a result of the short-lived advertising comparison. This is so because (1) Arkose is not an actual competitor of DataDome; (2) the comparison page had so little web traffic that DataDome took it down; and (3) DataDome’s potential customers are sophisticated and choose DataDome based on a free trial of the DataDome software.

To the extent that you believe the comparison page is functionally significant enough to cause harm, we note that Arkose published false and misleading claims about DataDome in its own comparison page. That page included more false statements than we can enumerate here, such as that DataDome lacks a challenge data feedback loop, use-case specific data and rule sets, active threat intel inputs, dynamic challenge capabilities, etc. This appears to be consistent with Arkose’s pattern and practice of aggressive, misleading, and false comparisons about Arkose’s actual and imagined competitors. DataDome fully intends to pursue federal, state, and common law counterclaims against Arkose for Arkose’s myriad false and misleading statements. We are aware that Arkose has disabled this website, but expect that this is purely for the optics of its lawsuit. Obviously, Arkose is obligated to preserve all documents in

Christian E. Mammen
February 23, 2024
Page 22

connection with all sales, marketing, advertising, and promotional statements about DataDome.

* * *

Simply put, there is no legitimate basis for Arkose to maintain any good faith and nonfrivolous claim of infringement or false advertising against DataDome and we demand that Arkose withdraw its allegations immediately. If Arkose refuses to drop its case notwithstanding being formally put on notice as to the frivolous nature of its claims, DataDome will seek attorneys' fees and other sanctions as the court may allow.

Sincerely,

/s/ Richard F. Martinelli