

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

VIDEOLABS, INC. and VL
COLLECTIVE IP LLC

Plaintiffs,

v.

META PLATFORMS, INC.;
INSTAGRAM, INC.; WHATSAPP
LLC; FACEBOOK TECHNOLOGIES,
LLC; and GIPHY, INC.

Defendants.

C.A. No. 22-cv-680-CFC

PLAINTIFF VIDEOLABS, INC. AND VL COLLECTIVE IP LLC'S
ANSWERING BRIEF OPPOSING DEFENDANTS'
PARTIAL MOTION TO DISMISS

Dated: August 29, 2022

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
FARNAN LLP
919 N. Market St., 12th Floor
Wilmington, DE 19801
Telephone: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Courtland L. Reichman (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
100 Marine Parkway, Suite 300
Redwood Shores, California 94065
Telephone: (650) 623-1401
Fax: (650) 623-1449

creichman@reichmanjorgensen.com

Christine E. Lehman (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
1710 Rhode Island Ave NW, 12th Floor
Washington, DC 20036
Telephone: (202) 894-7325
Fax: (650) 623-1449
clehman@reichmanjorgensen.com

Taylor N. Mauze (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
7500 Rialto Blvd., Ste. 1-250
Austin, Texas 78735
Telephone: (650) 623-1401
Facsimile: (650) 623-1449
tmauze@reichmanjorgensen.com

Wesley L. White (*pro hac vice*)
Jaime F. Cardenas-Navia (*pro hac vice*)
Michael Matulewicz-Crowley (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
750 Third Avenue, Suite 2400
New York, NY 10017
Telephone: (212) 381-1965
Facsimile: (650) 623-1449
wwhite@reichmanjorgensen.com
jcardenas-
navia@reichmanjorgensen.com
mmatulewicz-
crowley@reichmanjorgensen.com

*Attorneys for Plaintiffs VideoLabs, Inc.
and VL Collective IP LLC*

TABLE OF CONTENTS

I.	Nature And Stage Of Proceedings.....	1
II.	Summary of Argument	1
III.	Statement of Facts.....	2
A.	The '682 Patent Claims Innovate Transmission Of Real-Time Data.....	2
B.	The '980 Patent Claims Innovate Object Detection.....	4
IV.	Argument	7
A.	Legal Standards	7
B.	Meta Cannot Establish That The '682 Patent Is Ineligible As A Matter Of Law	9
1.	The '682 Patent Is Not Abstract.....	9
2.	If Reached, Meta Cannot Carry Its Burden At Step Two	14
C.	Meta Has Failed To Establish That The '980 Patent Is Ineligible As A Matter Of Law.....	15
1.	The '980 Patent Is Not Abstract.....	15
2.	If Reached, Meta's Step Two Arguments Fail.....	19
D.	Meta Has Failed To Carry Its Burden To Establish That Either Claim 1 Is Representative	19
E.	Videolabs Adequately Alleged Willful And Indirect Infringement ...	20
V.	Conclusion	22

TABLE OF AUTHORITIES

Page(s)

Federal Cases

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018)	7
<i>Alice Corp. Pty. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014).....	1, 8
<i>Ancora Techs., Inc. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018)	10, 12
<i>Automated Tracking Solutions, LLC v. Coca-Cola Co.</i> , 723 F. App’x 989 (Fed. Cir. 2018)	17
<i>Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Canada (U.S.)</i> , 687 F.3d 1266 (Fed. Cir. 2012)	18
<i>Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)	2, 15, 16
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)	7, 15
<i>Bozeman Fin. LLC v. Fed. Reserve Bank of Atlanta</i> , 955 F.3d 971 (Fed. Cir. 2020)	17
<i>Cellspin Soft, Inc. v. Fitbit, Inc.</i> , 927 F.3d 1306 (Fed. Cir. 2019)	7
<i>Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014)	17
<i>Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.</i> , 880 F.3d 1356 (Fed. Cir. 2018)	9
<i>CosmoKey Solutions GmbH & Co. KG v. Duo Sec. LLC</i> , 15 F.4th 1091 (Fed. Cir. 2021)	11, 15

<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	20
<i>Eko Brands, LLC v. Adrian Rivera Maynez Enters., Inc.</i> , 946 F.3d 1367 (Fed. Cir. 2020)	20
<i>Elec. Power Grp., LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016)	8, 17
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016)	8, 9
<i>Evolved Wireless, LLC v. Samsung Elecs. Co.</i> , 2016 WL 1019667 (D. Del. Mar.15, 2016)	21
<i>Finjan, Inc. v. Blue Coat Sys., Inc.</i> , 879 F.3d 1299 (Fed. Cir. 2018)	9, 12, 14
<i>Mgmt. Sci. Assocs., Inc. v. Datavant, Inc.</i> , 510 F. Supp. 3d 238 (D. Del. 2020).....	7, 13
<i>MONEC Holding AG v. Motorola Mobility, Inc.</i> , 897 F. Supp. 2d 225 (D. Del. 2012).....	22
<i>N. Star Innovations, Inc. v. Toshiba Corp.</i> , 2016 WL 7107230 (D. Del. Dec. 6, 2016)	22
<i>Packet Intelligence LLC v. NetScout Sys., Inc.</i> , 965 F.3d 1299 (Fed. Cir. 2020), <i>cert. denied</i> , 209 L. Ed. 2d 552 (Apr. 19, 2021).....	9, 11, 12
<i>Prism Techs. LLC v. T-Mobile USA, Inc.</i> , 696 F. App'x 1014 (Fed. Cir. 2017)	13
<i>RecogniCorp, LLC v. Nintendo Co.</i> , 855 F.3d 1322 (Fed. Cir. 2017)	19
<i>SAP Am., Inc. v. InvestPic, LLC</i> , 898 F.3d 1161 (Fed. Cir. 2018)	19
<i>Secured Mail Solutions LLC v. Universal Wilde, Inc.</i> , 873 F.3d 905 (Fed. Cir. 2017)	13, 14

<i>SRI Int’l, Inc. v. Cisco Sys., Inc.</i> , 930 F.3d 1295 (Fed. Cir. 2019)	<i>passim</i>
<i>TDE Petroleum Data Solutions, Inc., v. AKM Enter., Inc.</i> , 657 F. App’x 991 (Fed. Cir. 2016)	17
<i>TecSec, Inc. v. Adobe Inc.</i> , 978 F.3d 1278 (Fed. Cir. 2020)	11, 14, 20
<i>Thales Visionix Inc. v. United States</i> , 850 F.3d 1343 (Fed. Cir. 2017)	<i>passim</i>
<i>Universal Secure Registry LLC v. Apple Inc.</i> , 10 F.4th 1342 (Fed. Cir. 2021)	13, 14
<i>Universal Secure Registry LLC v. Apple Inc.</i> , 469 F. Supp. 3d 231 (D. Del. 2020).....	13
<i>VLSI Tech. LLC v. Intel Corp.</i> , 2019 WL 1349468 (D. Del. Mar. 26, 2019)	22
<i>ZapFraud, Inc. v. Barracuda Networks, Inc.</i> , 528 F. Supp. 3d 247 (D. Del. 2021).....	21
Federal Statutes	
35 U.S.C. § 101	1, 8, 9, 18
Federal Rules	
Rule 12	7, 13, 21

I. NATURE AND STAGE OF PROCEEDINGS

This is a patent case involving VideoLabs, Inc. and VL Collective IP LLC's ("VideoLabs") allegations that Meta Platforms, Inc., Instagram, Inc., Whatsapp LLC, Facebook Technologies, LLC, and Giphy, Inc. ("Meta") willfully infringe a portfolio of VideoLabs' critical video technology patents. Meta moved to dismiss-in-part, challenging that U.S. Patents 7,266,682 ("the '682 patent") and 7,436,980 ("the '980 patent") are ineligible for patenting, that indirect infringement is insufficiently alleged, and that Meta's infringement has not been willful. VideoLabs opposes.

II. SUMMARY OF ARGUMENT

1. Meta has failed to carry its burden to establish that the '682 and '980 patents are ineligible for patenting under 35 U.S.C. § 101 and *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208 (2014).

2. Both patents are eligible at step one of *Alice*, and the Court need not reach step two. The network authentication mechanism taught by the '682 patent presents a specific innovation in the transmission of real-time data over the internet that is eligible subject matter. Similarly, the '980 patent provides a concrete improvement to object detection in computer vision and is eligible.

3. If the Court reaches *Alice* step two for either patent, the record demonstrates VideoLabs' claims are inventive, as they comprise non-conventional

arrangements of elements that improve upon the prior art. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016).

4. Moreover, Meta fails to carry its burden to establish that either claim 1 is representative of all claims in each patent, and VideoLabs adequately pled willfulness and indirect infringement.

III. STATEMENT OF FACTS

5. Meta challenges the eligibility of only the '682 patent and the '980 patent. Both represent substantial research and development by Siemens, a major innovator in internet technology, including security and audio and visual transmission. D.I. 1 (“Compl.”) ¶¶61, 71. Innovation was key to Siemens’s business: in 2001 alone, it spent €6.6 billion on research and development. *Id.*

A. The '682 Patent Claims Innovate Transmission Of Real-Time Data

6. The '682 patent addresses a longstanding problem in the transmission of real-time audio and visual data over the internet. In the mid-1990s, the Real Time Transport Protocol, or RTP, was developed by the IETF, designed for end-to-end real-time transfer of streaming media. Compl. ¶¶62–63. RTP was based on “application-layer framing,” where functions were implemented in the application layer as opposed to the computer’s operating system protocol stack. *Id.* ¶63.

7. But RTP was not very secure. *Id.* at ¶64. Transmission networks carrying RTP payload packets were susceptible to security flaws at the transmitter,

during transmission, and at the receiver. *See* '682 patent 2:44–3:10. Attackers could overload the network—sending mass data to receivers, encumbering availability and performance. *Id.* 2:47–64. Firewalls were of limited use because it was a “simple matter for an attacker to send [its] meaningless (mass) data to addresses within the private network as well, that is to say, behind the firewall.” *Id.* 2:65–3:10.

8. In one approach, the IPSEC protocol, “data packets of the Internet protocol (IP data packets) [could] be encapsulated and [could] be protected in terms of confidentiality and/or integrity.” *Id.* 3:21–23. It included a cookie-based mechanism, linking fast one-way hash functions, random numbers, and IP addresses to one another. *Id.* 3:16–41. But that solution had a security gap: the “first ‘cookie’ transmitted from the transmitter to the receiver” was unprotected. *Id.* 3:30–34. And the cookie method could not ensure protection against unwanted mass data on the application layer under real-time conditions. *Id.* 3:34–38. Structurally, it was not possible to link IPSEC to the security functions of an application. *Id.* 3:38–41.

9. Ultimately, IETF introduced a security and authentication layer into RTP in 2004 called SRTP. Compl. ¶¶65 & n.23.

10. But years before the formalization and publication of SRTP, the '682 patent inventors had already recognized and solved RTP's security problems. Compl. ¶¶66. The '682 patent captures, at least in part, performing SRTP/SRTCP authentication practices using the WebRTC standard. Compl. ¶¶234–41.

11. The '682 patent teaches an improved network-security mechanism. The transmitter is used to insert authentication data into the data packets *before* the packets are transmitted. *Id.*; '682 patent 3:45–52, 7:6–10. The authentication data is then transmitted with the data packet and analyzed by the receiver to ensure that the receiver knows the transmitter or vice versa; if the receiver and transmitter do not know each other, the data is rejected but if they do, the data is processed. *Id.*; '682 patent Fig. 3, 3:49–54, 5:32–36, 7:6–21. This process is reflected both in the specification and the claim language itself. *See, e.g.*, '682 patent 7:55–67 (claim 1 setting forth the above steps).

12. Authenticating in the application layer as described in the patent is extremely advantageous from both a user and network perspective. Compl. ¶¶68–69. It reduces the size of authentication data, '682 patent 3:60–4:10; 7:30–34, increases the transmission system's performance, reduces the implementation complexity of the system, provides real-time availability of data, and avoids the need for buffering or loading, *see id.* 4:7–9.

B. The '980 Patent Claims Innovate Object Detection

13. The '980 patent takes aim at a different problem: object detection in computer vision. Compl. ¶72. The patented improvement in computer vision is not about identifying an existing practice (vision) and saying, “do it on a computer.”

Instead, the '980 patent teaches a specific technique that improves the accuracy with which computers detect and track objects in digital images. *Id.* ¶¶72–74.

14. At the time of the invention, existing computer vision solutions performed poorly when identifying or tracking objects when image conditions were not pristine, such as when objects are partially covered, rotated, scaled, or otherwise distorted. Compl. ¶73.

15. To address these problems, the inventors added, *inter alia*, a time dimension to computer vision modeling. For example, while object detection may be difficult when an object is partly obscured, if the detection of that image in preceding and/or succeeding images is also integrated into the analysis, then the model can more accurately predict the presence of the object. D.I 1-5 ('980 patent) Figs. 2A, 2B, 2:43–54, 4:34–37, 7:56–8:17; Compl. ¶74. The '980 patent's spatio-temporal model takes advantage of additional information and relationships across time to improve object detection and tracking, which was previously unknown. *Id.* (citing D.I. 1-26, 1-28).

16. When the inventors compared the patented spatio-temporal model with a prior-art detection technique under real-world conditions, “[t]he spatio-temporal object model consistently combine[d] the evidence for accurate estimates throughout the sequence,” while the prior art technique’s performance was “poor.” '980 patent, 7:56–8:17.

17. The '980 patent's spatio-temporal model is a graphical model with nodes that correspond to each of the collection of components and to the object. *Id.* 1:41–42. “Each node in the graph represents either the object or a component of the object at time *t*.” *Id.* 3:47–50. Essentially, an object (*e.g.*, a pedestrian) and the components of that object are mapped using both “the temporal compatibility of object state between frames” (*i.e.*, its state from second to second) and “the spatial compatibility of the object and its components” within a single frame. Compl. ¶75.

18. The patent also describes a two-layer model, Compl. ¶76, with object and component layers. For a pedestrian, the components might be the head, the left arm, the right arm, and the legs. The component layer would be made up of nodes corresponding to those components, while the object layer is just the object—the pedestrian. *Id.* “Having a two-layer graphical model allows the inference process to reason explicitly about the object as a whole . . . and reduce the complexity of the graphical model by allowing the assumption of the conditional independence of components.” '980 patent 4:37–41. In addition to speeding up object detection, the patented method “facilitates detection of complex articulated objects as well as helps in handling partial object occlusions or local illumination changes.” *Id.* 2:51–54.

19. Each of these interrelated features—the spatio-temporal model, the probability analysis, and the two-layered approach—are reflected in the claim language. *See, e.g.*, '980 patent 8:30–43 (claim 1).

IV. ARGUMENT

A. Legal Standards

At Rule 12(b)(6), the Court accepts as true all factual allegations in the complaint and in documents explicitly relied upon in the complaint and views them in the light most favorable to the nonmovant. *See, e.g., Mgmt. Sci. Assocs., Inc. v. Datavant, Inc.*, 510 F. Supp. 3d 238, 244 (D. Del. 2020); *Umland v. Planco Fin. Servs.*, 542 F.3d 59, 64 (3d Cir. 2008).

“Whether a claim recites patent eligible subject matter is a question of law which may contain disputes over underlying facts.” *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). While eligibility can be determined at Rule 12(b)(6), “[t]his is only true when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law.” *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018). “[P]lausible and specific factual allegations that aspects of [a] claim[] are inventive are sufficient” at the Rule 12 stage. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1317 (Fed. Cir. 2019).

The Supreme Court has provided “a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.” *Alice*, 573 U.S. at 217. “First, we determine whether the claims at issue are directed to one of those patent-

ineligible concepts,” and, “[i]f so, we then ask, ‘what else is there in the claims before us?’” *Id.* (cleaned up). To answer that second question, courts “consider the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Id.* “While the two steps of the *Alice* framework are related, the ‘Supreme Court’s formulation makes clear that the first-stage filter is a meaningful one, sometimes ending the § 101 inquiry.’” *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1346 (Fed. Cir. 2017) (quoting *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016)).

While at first glance eligibility law can be difficult to navigate, one clear, reliable rule has emerged in the cases: Claims that are “directed to a specific improvement to computer functionality” or “to a specific implementation of a solution to a problem in the software arts” are not directed to an abstract idea. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1338-39 (Fed. Cir. 2016). Indeed, the Federal Circuit routinely holds “claims focused on various improvements of systems directed to patent eligible subject matter under § 101.” *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1362 (Fed. Cir. 2018) (collecting cases). In *Enfish*, claims to a self-referential table in a computer database were eligible because they improved a computer’s functionality. In *Thales*, claims that “specif[ied] a particular configuration of inertial sensors and a

particular method of using the raw data from the sensors in order to more accurately calculate the position and orientation of an object on a moving platform” were eligible at step one. 850 F.3d at 1349. In *Finjan*, a claim to a modified file that enabled security systems to do things they could not previously was eligible at step one. *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1305 (Fed. Cir. 2018). In *Packet Intelligence*, claims reciting specific steps to refine data flow in a network environment were eligible at step one because the purported invention addressed shortcomings in the art and generated a more granular, nuanced, and useful classification of network traffic. *Packet Intelligence LLC v. NetScout Sys., Inc.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020). The court in *SRI* similarly upheld claims directed to a “specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network.” *SRI Int’l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019).

B. Meta Cannot Establish That The ’682 Patent Is Ineligible As A Matter Of Law

1. The ’682 Patent Is Not Abstract

Claim 1 offers a specific technique to solve the computer-only problem of security and authentication problems in network-based audio and visual streaming. *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018)

(“Improving security . . . against a computer’s unauthorized use of a program—can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem.”). Precedent is replete with examples of similar, eligible network-security innovations.

SRI is the cornerstone of that precedent. There, the patent was directed to a “computer-automated method of hierarchical event monitoring” where network monitors detected suspicious activity on a network and generated reports. *SRI*, 930 F.3d at 1301. As Meta does here, Cisco asserted that the claims were simply directed to analyzing data from multiple sources to detect suspicious activity, running afoul of *Electric Power* and similar cases. *Id.* at 1303–04. But the Federal Circuit disagreed: the *SRI* claims prevented the “normal, expected operation of a conventional computer network,” overriding that sequence of events and replacing it with the claimed detection mechanism. *Id.* at 1304. Instead of using a computer as tool, the computer’s technical function was improved with a specific technique for improving network security. *Id.*

Similarly, in *Packet Intelligence*, claims to network monitoring where packets of data passing over a network were checked against existing “flows” and entered into a “flow-entry database” to aid in network data classification were held eligible. 965 F.3d at 1304. The court relied on the specification’s teachings that

the claims provided a “more granular, nuanced, and useful classification of network traffic,” an improvement in computer technology. *Id.* at 1309–10.

The claims in *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1295 (Fed. Cir. 2020), which allowed for the simultaneous transmission of secure information to a large group of recipients connected to a decentralized network—an important feature of data networks—permitting different levels of access for different users, were held eligible at step one. The *TecSec* invention relied on encryption and data labeling to “improv[e] a basic function of a computer data-distribution network, namely, network security.” *Id.* at 1295–96.

The ’682 patent presents a similarly patent-eligible innovation: claim 1 is directed to a specific network-verification method that, based on the specification, “depart[s] from earlier approaches and improve[s] computer technology,” *CosmoKey Solutions GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091, 1096 (Fed. Cir. 2021); Facts ¶¶6–11. Such innovations are patent eligible. *Id.* at 1099 (specific, improved method for network security that turned authentication on and off automatically eligible); *see also Finjan*, 879 F.3d at 1305 (a security-profile approach to network security, where virus-scan information was appended to a file to warn recipients and restrict access eligible).

The ’682 claims, like those in *SRI*, improve computer function by providing a specific technique for improving network security. *Ancora*, 908 F.3d at 1348;

Facts ¶¶6–12. RTP transmission was known to be unsecure and, to the extent authentication was possible, that authentication was not at the application layer. *See* Facts ¶¶7–9. Claim 1 prescribes a communication mechanism between RTP transmitters and receivers whereby the receiver and transmitter authenticate each other at the application layer *before* data is accepted and authentication data is inserted at the end of a whole RTP packet payload. ’682 patent 7:7:55–67; Facts ¶¶10–11. This avoids the security pitfalls described in the specification because, at the transmitter, authentication data is inserted into a data packet before transmission, and the receiver and transmitter can ensure that they know one another before data was processed. ’682 patent 7:7:55–67; Facts ¶11. The patent provides a new way of organizing network traffic like that in *Packet Intelligence*, and, like *TecSec*’s labeling and encryption of data, these claims improve computer technology and solve a problem unique to computer networks: preventing unauthorized data access and improving network security. Facts ¶¶11–12. It is likely these benefits led to widespread adoption of the ’682 patent’s improved authentication practices; VideoLab’s invention is now the standard. *See* Compl. ¶¶234–41; Facts ¶¶9–12.

Meta sidesteps these cases, instead relying on *Prism*, *USR*, and *Secured Mail* to argue that the claims “apply conventional authentication,” and are directed to “ensuring that [transmitted] data are not unwanted data,” Meta Br. 9. To accept

Meta’s framing would be to credit its argument over the detailed factual allegations in the specification and Complaint. But that leap is not permitted at Rule 12(b)(6) where the facts pled in the Complaint and provided in the specification are to be taken as true. *Mgmt. Sci. Assocs.*, 510 F. Supp. 3d at 244.

Nevertheless, Meta’s cases do not resemble the ’682 patent. The *Prism* claims were directed to the abstract idea of “providing restricted access to resources,” requiring nothing more than receiving identity data, confirming its authenticity, and letting authorized access through. *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App’x 1014, 1017 (Fed. Cir. 2017). The key failing of the *Prism* claims was a lack of “concrete, specific solution,” opting for “generic steps typical of any conventional process for restricting access, including processes that predated computers.” *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1347 (Fed. Cir. 2021) (describing *Prism*). This Court relied on *Prism* in its opinion holding the *USR* claims ineligible. *Universal Secure Registry LLC v. Apple Inc.*, 469 F. Supp. 3d 231, 237 (D. Del. 2020). Those claims, like that in *Prism*, were directed to a similar series of steps for authorizing access to data. And the Federal Circuit agreed that the *USR* claims were directed to an abstract idea, “simply recit[ing] conventional actions in a generic way” without “purport[ing] to improve any underlying technology.” *USR*, 10 F.4th at 1349.

But here, the claims provide a concrete solution not used in the art—inserting

authentication data at the transmitter at the end of an RTP data payload and having the receiver and transmitter confirm they know each other before decoding the data. Facts ¶¶9–12. The patent does not recite “conventional actions in a generic way,” instead prescribing a specific mechanism of receiver and transmitter communication to authenticate the data exchange, a key innovation in the art that became part of the standard. *See* Facts ¶¶6–12.

Secured Mail is inapposite. There, the patentee proposed marking mail items with “unique identifier[s],” such as sender and recipient information. *Secured Mail Solutions LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 910–11 (Fed. Cir. 2017). Mail marking is certainly not an issue unique to computer networks, so this case is of little relevance. Nonetheless, Meta overextends *Secured Mail*, arguing claims that “append authentication data to known message types” are ineligible, Meta Br. 10, ignoring that the *Finjan* claims were eligible when security information was appended to files transmitted over a network, 879 F.3d at 1305, as were the labels and authentication in *TecSec*, 978 F.3d at 1295–96.

2. If Reached, Meta Cannot Carry Its Burden At Step Two

Because the ’682 patent claims are not directed to an abstract idea, the Court need not reach step two. *Thales*, 850 F.3d at 1346.

But even accepting Meta’s view that the claims are directed to ensuring transmitted data is not unwanted, the claims recite a specific improvement to

conventional audio and video streaming by using more secure authentication method that prevents unauthorized access and attacks. *See* Facts ¶¶6–12. That is a “technical solution to a security problem in networks and computers,” *CosmoKey*, 15 F.4th at 1098, and there is nothing in the specification or complaint suggesting that the claim elements as an ordered combination are conventional. Instead, as in *CosmoKey*, the specification explains how the claims as a whole are inventive. *See* Facts ¶¶6–12.

To be sure, the ’682 patent does not suggest that it invented new cryptographic algorithms or new physical computer components. But that is not required. “The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional.” *Berkheimer*, 881 F.3d at 1369. “[A]n inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces.” *Bascom*, 827 F.3d at 1350.

C. Meta Has Failed To Establish That The ’980 Patent Is Ineligible As A Matter Of Law

1. The ’980 Patent Is Not Abstract

The ’980 patent offers a separate technological improvement: optimized computer vision with object detection. *See* Facts ¶¶13–19. Central to the claims is use of a “spatio-temporal model,” a “graphical model comprising nodes corresponding to each of the collection of components and to the object,” which maps objects and their components using the objects’ state over time and their spatial

compatibility. Facts ¶¶17–19; ’980 patent 1:40–43. Use of the spatio-temporal model as claimed yields a significant benefit over existing methods. *See* ’980 patent 7:56–8:17. The claimed method speeds up object detection and is particularly effective in detecting overlapping components or light changes within an image. *See* Facts ¶¶13–19. The claims are not directed to computer vision “writ large,” but instead, a specific, non-abstract improvement. *Id.*

Thales provides a close analogy. In *Thales*, the Federal Circuit considered an invention for determining object orientation relative to a moving reference frame based on signals from two inertial sensors. 850 F.3d at 1345. The claims specified a particular configuration of sensors and method of using the sensor data “to more accurately calculate the position and orientation of an object on a moving platform,” and were not directed to an abstract idea. *Id.* at 1349.

Just so here. The ’980 claims rely on a spatio-temporal model with a series of nodes representing the object or a component of that object at time *t*; objects and their components are mapped over time to determine the probability that an object is present. Facts ¶¶17–19. The particular nodes, like the sensors in *Thales*, collect specific data that the claims process into more accurate object detection. *See, e.g., id.*; ’980 patent 3:49–4:7, claim 1.

Meta does not address *Thales*. Instead, it relies on *Electric Power* and similar cases, argues that the claims use human concepts combined with math, and suggests that the claims do not solve a technological problem.

But the *Electric Power* claims were drawn to analyzing, collecting, and detecting information *about a power grid*—using computers as a tool to solve non-technological power-grid problem. 830 F.3d at 1354; *see also SRI*, 930 F.3d at 1304. Collecting and processing data to solve non-technological problems, such as processing hard-copy documents, *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1345 (Fed. Cir. 2014), fraud detection in check-cashing, *Bozeman Fin. LLC v. Fed. Reserve Bank of Atlanta*, 955 F.3d 971, 978–79 (Fed. Cir. 2020), and oil-well operation, *TDE Petroleum Data Solutions, Inc., v. AKM Enter., Inc.*, 657 F. App’x 991, 993 (Fed. Cir. 2016), are abstract. But the ’980 claims do not seek to analyze data to solve a business problem or automate a tracking method, *Automated Tracking Solutions, LLC v. Coca-Cola Co.*, 723 F. App’x 989, 994 (Fed. Cir. 2018), and these cases are inapposite. The problem solved here does not exist outside of the realm of computers.

The claim also does not seek to “‘automate’ human vision.” Meta Br. 15. As a threshold matter, it is not clear that automating anything humans are capable of—like vision or other bodily functions—are ineligible inventions. For example, the human body produces insulin, but no one would seriously contend that an insulin

pump is ineligible for patenting. Regardless, Meta is incorrect. The claim uses a *specific* model and set of components to provide an improved simulation of object recognition, offering an inventive solution that is reliable for obscured and overlapping objects and for images in varying lighting conditions. *See* Facts ¶¶13–19. This is achieved through the spatio-temporal model, node measurements, and probability calculations. *Id.*

Puzzlingly, Meta also suggests that the claims do not *use* the spatio-temporal model. Claim 1’s steps expressly use the model. *See id.*; ’980 patent 8:30–43 (claiming providing a video, measuring the object as a collection of components, determining the probability that the object is in each image, and detecting the object). To the extent the scope of the claims is at issue, resolution of eligibility without claim construction would be inappropriate, and this motion should be deferred until after *Markman*. *See Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Canada (U.S.)*, 687 F.3d 1266, 1273–74 (Fed. Cir. 2012) (“[I]t will ordinarily be desirable—and often necessary—to resolve claim construction disputes prior to a § 101 analysis, for the determination of patent eligibility requires a full understanding of the basic character of the claimed subject matter.”).

Meta also relies on *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017), but this claim is not directed to encoding and decoding data; instead, particular nodes collect specific data and generate more accurate object

detection using the spatio-temporal model, Facts ¶¶17–18, like the *Thales* claim. *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1168 (Fed. Cir. 2018), and the like are similarly irrelevant because “focus of [these] claims” is an “improved . . . network,” Facts ¶¶13–19.

Ultimately, Meta’s position that “the claims merely implement commonplace human concepts and mathematical algorithms” proves too much: that reasoning would likely render ineligible any computer vision patent, including some of Meta’s own. *See, e.g.*, U.S. Patent 10,713,794 (“computer vision” patent on “object detection and segmentation in images”).

2. If Reached, Meta’s Step Two Arguments Fail

For the analogous reasons described *supra* for the ’682 patent, the Court need not reach step two, but, if it does, step two is readily met. Additionally, Meta cannot refute the allegation the spatio-temporal model used in the ’980 patent is unconventional alone and in combination with the other claim limitations.

D. Meta Has Failed To Carry Its Burden To Establish That Either Claim 1 Is Representative

Next, Meta urges dismissal of the ’682 and ’980 patent allegations if claim 1 of each patent is treated as representative. Not so. As identified above, the components of each patent are unconventional alone or in combination. *See* Facts ¶¶6–19. The ’682 claims, for example, need not include a new form of authentication and transmission to provide an unconventional arrangement of those

components. For the '980 claims, Meta offers a watered-down anticipation or obviousness analysis, suggesting that combining what it deems are “known” elements is conventional. But absent from its analysis is any consideration that the ordered combination of those limitations with the elements in claim 1 or the other independent claims is conventional. *See, e.g., DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1259 (Fed. Cir. 2014).

E. Videolabs Adequately Alleged Willful And Indirect Infringement

Finally, Meta seeks sweeping dismissal of willfulness and indirect infringement claims for all patents-in-suit. Willful infringement is intentional or deliberate. *Eko Brands, LLC v. Adrian Rivera Maynez Enters., Inc.*, 946 F.3d 1367, 1378 (Fed. Cir. 2020). “The intent standard focuses on, and can be met by proof of, the defendant’s subjective state of mind, whether actual knowledge or the subjective beliefs (coupled with action to avoid learning more) that characterizes willful blindness.” *TecSec*, 978 F.3d at 1286.

The allegations in the Complaint represent Meta’s actual knowledge and avoidance to learning more. VideoLabs reached out to Meta years before filing the instant Complaint, culminating in an in-person meeting and multiple communications about VideoLabs’ portfolio. VideoLabs even notified Meta that it had 17 unique claim charts mapping out Meta’s infringement for discussion. VideoLabs reasonably alleged that Meta would have investigated post-

communication. *See, e.g.*, Compl. ¶¶140–43; 178–181; 221–224; 243–246; 269–272. Meta does not dispute these allegations (apart from calling one “baseless”). Meta Br. 24. Further, VideoLabs sent Meta a letter pre-suit that expressly notified Meta of its infringement of the patents-in-suit. Compl. ¶¶141, 179, 222, 244, 270.

Knowledge is about *Meta’s* state of mind, and VideoLabs cannot provide (without discovery) direct evidence conclusively establishing Meta’s intentions. But that is not the standard. At Rule 12, the Court takes well-pled allegations as true and resolves inferences in favor of VideoLabs. From these meetings, communications, and likely investigations, considered together, a factfinder could infer Meta’s intentional and inducement of infringement. The sum of the allegations here is markedly different than the threadbare ones in Meta’s cases. *See, e.g., ZapFraud, Inc. v. Barracuda Networks, Inc.*, 528 F. Supp. 3d 247, 252 (D. Del. 2021) (dismissing willfulness claims “based solely” on the complaint); *Evolved Wireless, LLC v. Samsung Elecs. Co.*, 2016 WL 1019667, at *3–5 (D. Del. Mar.15, 2016) (no pre-suit knowledge when pre-suit letter included a list of 85 *patents* without specifically highlighting the patents-in-suit); *MONEC Holding AG v. Motorola Mobility, Inc.*, 897 F. Supp. 2d 225, 231 (D. Del. 2012) (rejecting allegation that defendants would know about a patent by monitoring the litigation activities of competitors who had been sued for infringement); *VLSI Tech. LLC v. Intel Corp.*, 2019 WL 1349468, at *2 (D. Del. Mar. 26, 2019) (rejecting knowledge based on

complaint). VideoLabs’ allegations about the Meta Companies include that the Meta Companies are “heavily intertwined” with respect to the infringing products, *see, e.g.*, Compl. ¶17, in contrast to the vague allegations in *N. Star Innovations, Inc. v. Toshiba Corp.*, 2016 WL 7107230, at *2 (D. Del. Dec. 6, 2016).

To the extent VideoLabs’ allegations do not put Meta on adequate notice, VideoLabs requests leave to amend its Complaint.

V. CONCLUSION

VideoLabs requests that the Court deny Meta’s motion.

Dated: August 29, 2022

Respectfully submitted,

FARNAN LLP

/s/ Michael J. Farnan
Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market St., 12th Floor
Wilmington, DE 19801
Telephone: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Courtland L. Reichman (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
100 Marine Parkway, Suite 300
Redwood Shores, California 94065
Telephone: (650) 623-1401
Fax: (650) 623-1449
creichman@reichmanjorgensen.com

Christine E. Lehman (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
1710 Rhode Island Ave NW, 12th
Floor
Washington, DC 20036
Telephone: (202) 894-7325
Fax: (650) 623-1449
clehman@reichmanjorgensen.com

Taylor N. Mauze (*pro hac vice*)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
7500 Rialto Blvd., Ste. 1-250
Austin, Texas 78735
Telephone: (650) 623-1401
Facsimile: (650) 623-1449
tmauze@reichmanjorgensen.com

Wesley L. White (*pro hac vice*)
Jaime F. Cardenas-Navia (*pro hac*
vice)
Michael Matulewicz-Crowley (*pro hac*
vice)
REICHMAN JORGENSEN LEHMAN
& FELDBERG LLP
750 Third Avenue, Suite 2400
New York, NY 10017
Telephone: (212) 381-1965
Facsimile: (650) 623-1449
wwhite@reichmanjorgensen.com
jcardenas-
navia@reichmanjorgensen.com
mmatulewicz-
crowley@reichmanjorgensen.com

*Attorneys for Plaintiffs VideoLabs, Inc.
and VL Collective IP LLC*

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing filing contains 4,994 words, in compliance with the 5,000 word-count limit provided in the Court's Standing Order Regarding Briefing In All Cases. The undersigned further certifies that the foregoing complies with the font/typeface requirements of the same and is typed in 14-point, Times New Roman typeface.

Date: August 29, 2022

/s/ Michael J. Farnan
Michael J. Farnan (Bar No. 5165)