IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

CARBYNE BIOMETRICS, LLC, **Plaintiff,** **vs.** **APPLE INC.,** **Defendant.**	**Civil Action No. 1:23-cv-00324** **JURY TRIAL**

DEFENDANT'S RULE 12(B)(6) MOTION TO DISMISS THE COMPLAINT FOR FAILURE TO STATE A CLAIM UNDER 35 U.S.C. § 101

TABLE OF CONTENTS

I. INTRODUCTION 1

II. LEGAL STANDARD 2

III. THE FRAUD REDUCTION PATENTS CLAIM INELIGIBLE SUBJECT MATTER 3

A. Background of the Fraud Reduction Patents and Their Exemplary Claims 3

B. Step One: The Fraud Reduction Patents are Directed to an Abstract Idea 6

C. Step Two: The Fraud Reduction Patents Lack Any Inventive Concept 10

IV. THE AUTHENTICATION PATENTS CLAIM INELIGIBLE SUBJECT MATTER 12

A. Background of the Authentication Patents and Their Exemplary Claims 12

B. Step One: The Authentication Patents are Directed to an Abstract Idea 15

C. Step Two: The Authentication Patents Lack Any Inventive Concept 18

V. NO ADDITIONAL FACT FINDING IS NECESSARY TO DECIDE THIS MOTION 20

VI. DISMISSAL WITH PREJDUCE WARRANTED 20

TABLE OF AUTHORITIES

Page(s)

Cases

Affinity Labs v. Amazon.com Inc.,
838 F.3d 1266 (Fed. Cir. 2016).....12, 19

Affinity Labs v. DirectTV, LLC,
838 F.3d 1253 (Fed. Cir. 2016).....11

Alice Corp. Pty. v. CLS Bank Int'l,
573 U.S. 208 (2014)..... *passim*

Apple Inc. v. Ameranth, Inc.,
842 F.3d 1229 (Fed. Cir. 2016).....2

AuthWallet, LLC v. Block, Inc.,
602 F. Supp. 3d 620 (S.D.N.Y. 2022), *aff'd sub nom. In re AuthWallet, LLC*,
No. 2022-1842, 2023 WL 3330298 (Fed. Cir. May 10, 2023).....10

Bilski v. Kappos,
561 U.S. 593 (2010).....3

Blue Spike, LLC v. Google Inc.,
No. 14-cv-01650, 2015 WL 5260506 (N.D. Cal. Sept. 8, 2015),
aff'd, 669 F. App'x 575 (Fed. Cir. 2016).....8, 9, 17

BSG Tech LLC v. Buyseasons, Inc.,
899 F.3d 1281 (Fed. Cir. 2018).....10

Coho Licensing LLC v. Glam Media, Inc.,
2017 WL 6210882 (N.D.Cal., 2017) *aff'd sub nom. Coho Licensing LLC v. Oath Inc.*, 710 F. App'x. 892 (Fed. Cir. 2018).....19

CyberSource Corp. v. Retail Decisions, Inc.,
654 F.3d 1366 (Fed. Cir. 2011).....2, 9, 16

Data Engine Tech. LLC v. Google LLC,
906 F.3d 999 (Fed. Cir. 2018).....6

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014).....9, 11, 16, 20

Electric Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016).....2, 7, 16, 17

Electronic Commc'n Techs., LLC v. ShoppersChoice.com, LLC,
958 F.3d 1178 (Fed. Cir. 2020).....18

Enfish, LLC v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016).....9

FairWarning IP, LLC v. Iatric Sys., Inc.,
839 F.3d 1089 (Fed. Cir. 2016)..... *passim*

Front Row Techs., LLC v. NBA Media Ventures, LLC,
204 F. Supp. 3d 1190 (D.N.M. 2016), *aff'd sub nom. Front Row Techs., LLC v. MLB Adv'd Media, L.P.*, 697 F. App'x 701 (Fed. Cir. 2017) 8

GeoComply Sols. Inc. v. Xpoint Servs. LLC,
No. 22-1273, 2023 WL 1927393 (D. Del. Feb. 10, 2023).....8

Intellectual Ventures I LLC v. Capital One Bank (USA),
792 F.3d 1363 (Fed. Cir. 2015).....20

Intellectual Ventures I LLC v. Erie Indem. Co.,
850 F.3d 1315 (Fed. Circ. 2017)..... *passim*

Legate v. Livingston,
822 F.3d 207 (5th Cir. 2016) 20

Marucci Sports, L.L.C. v. NCAA,
751 F.3d 368 (5th Cir. 2014) 3

Maxon, LLC v. Funai Corp.,
726 F. App'x 797 (Fed. Cir. 2018) 19

Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.,
811 F.3d 1314 (Fed. Cir. 2016).....18

NEXRF Corp. v. Playtika Ltd.,
547 F. Supp. 3d 977 (D. Nev. 2021), *aff'd*, 2022 WL 1513310
(Fed. Cir. May 13, 2022) 8

RecogniCorp, LLC v. Nintendo Co.,
855 F.3d 1322 (Fed. Cir. 2017).....2, 17, 18

SAP Am., Inc. v. Investpic, LLC,
898 F.3d 1161 (Fed. Cir. 2018).....3, 19

Sensormatic Elecs., LLC v. Wyze Labs, Inc.,
484 F. Supp. 3d 161 (D. Del. 2020), *aff'd*, 2021 U.S. App. LEXIS 20789 (Fed. Cir. July 14, 2021) 19

Solutran, Inc. v. Elavon, Inc.,
931 F.3d 1161 (Fed. Cir. 2019).....7, 16

Umbanet, Inc. v. Epsilon Data Mgmt., LLC,
263 F. Supp. 3d 647 (E.D. Tex. 2017), *aff'd*, 745 F. App'x
168 (Fed. Cir. 2018).....17

United States v. St. Luke's Episcopal Hosp.,
355 F.3d 370 (5th Cir. 2004) 20

WhitServe LLC v. Dropbox, Inc.,
854 F. App'x 367 (Fed. Cir. 2021) 17, 18, 19

Yu v. Apple Inc.,
1 F.4th 1040 (Fed. Cir. 2021) ..... *passim*

Statutes

35 U.S.C. § 101..... *passim*

TABLE OF ABBREVIATIONS

Term	Definition
Apple	Defendant Apple Inc.
Carbyne	Plaintiff Carbyne Biometrics, LLC
’512	U.S. Patent No. 10,929,512
’105	U.S. Patent No. 11,475,105
’138	U.S. Patent No. 11,514,138
’010	U.S. Patent No. 9,972,010
’656	U.S. Patent No. 10,713,656
’886	U.S. Patent No. 11,526,886
Fraud Reduction Patents	The ’010, ’656, and ’886 patents
Fraud Reduction Claims	Claims 1, 5-6, 9, 13-14, 17, and 21-22 of the ’010 Patent; claims 1, 4, 7-10, 13, and 16-19 of the ’656 Patent, and claims 1-2, 4-7, 9-11, 12, 14, 18, and 20 of the ’886 Patent
Authentication Patents	The ’512, ’105, and ’138 patents
Authentication Claims	Claims 1, 3, 7-8, 10-13, 15, 19, and 22-25 of the ’138 Patent, claims 1, 9, 11, 18, 28, and 35 of the ’105 Patent, and claims 1-4, 10-14, and 20-21 of the ’512 Patent
Asserted Patents	The ’512, ’105, ’138, ’010, ’656, and ’886 patents
Recited Claims	The Fraud Reduction Claims and Authentication Claims
’010 FH	Excerpt from the File History to U.S. Patent No. 9,972,010
’886 FH	Excerpt from the File History to U.S. Patent No. 11,526,886
Brief	Corrected Principal And Response Brief For Defendant/Cross-Appellant T-Mobile USA, Inc. at 58-59, *Prism Technologies LLC v. T-Mobile USA, Inc.*, Nos. 16-2031, 16-2049 (Fed. Cir.) (filed Sept. 22, 2016)

TABLE OF EXHIBITS

Exhibit	Document
Ex. A	U.S. Patent No. 10,929,512 (attached as Exhibit A to the Complaint)
Ex. B	U.S. Patent No. 11,475,105 (attached as Exhibit B to the Complaint)
Ex. C	U.S. Patent No. 11,514,138 (attached as Exhibit C to the Complaint)
Ex. D	U.S. Patent No. 9,972,010 (attached as Exhibit D to the Complaint)
Ex. E	U.S. Patent No. 10,713,656 (attached as Exhibit E to the Complaint)
Ex. F	U.S. Patent No. 11,526,886 (attached as Exhibit F to the Complaint)
Ex. G	Excerpt from the File History of U.S. Patent No. 9,972,010, retrieved from the website of the U.S. Patent and Trademark Office
Ex. H	Excerpt from the File History of U.S. Patent No. 11,526,886, retrieved from the website of the U.S. Patent and Trademark Office
Ex. I	Corrected Principal And Response Brief For Defendant/Cross-Appellant T-Mobile USA, Inc. at 58-59, *Prism Technologies LLC v. T-Mobile USA, Inc.*, Nos. 16-2031, 16-2049 (Fed. Cir.) (filed Sept. 22, 2016)

I. INTRODUCTION

Carbyne asserts six patents that claim patent ineligible subject matter under 35 U.S.C. § 101. Each Recited Claim[1] is analogous to claims the Federal Circuit has determined are abstract in controlling cases, and none recites anything inventive—such as new components, or technological improvements to conventional components—that might transform them into reciting patent-eligible subject matter. Instead, the Recited Claims are written in functional terms, setting forth a desired result instead of a particular solution for achieving that result. To the extent they recite tangible components at all, the Recited Claims recite only conventional components performing only their conventional functions (*e.g.*, processors accessing data). Accordingly, the Court should dismiss the complaint, with prejudice, for failure to state a claim.

The Asserted Patents fall into two technical groups, neither of which is patent-eligible:

Fraud Reduction: The ’010, ’656, and ’886 patents are directed to the abstract idea of collecting, receiving, and analyzing information about a user to enable a transaction. The claims are indistinguishable from, and indeed broader than, the claims the Federal Circuit found patent-ineligible in *Universal Secure Registry LLC v. Apple Inc.*, which were directed to “collect[ing] and examin[ing] data to authenticate the user’s identity.” 10 F.4th 1342, 1352 (Fed. Cir. 2021) (“*USR*”). The claims here recite the same abstract steps as those in *USR*, namely collecting and receiving biometric information from a user and examining whether to proceed with a transaction based on the collected information. The claims here also similarly contain no inventive concept, as they describe merely implementing the abstract idea on conventional computer systems.

Authentication: The ’138, ’105, and ’512 patents are directed to the abstract idea of facilitating access to resources based on authenticating a user’s identity. They are indistinguishable

[1] Definitions may be found in the Table of Abbreviations. Emphasis added unless otherwise noted.

from those held ineligible in *Prism Technologies LLC v. T-Mobile USA, Inc.*, which were directed to "control[ling] access to . . . computer resources by authenticating identity data." 696 F. App'x 1014, 1016 (Fed. Cir. 2017) (non-precedential). Indeed, they recite the same steps as in *Prism*, *i.e.*, receiving identity data and an access request, determining if access is authorized, and enabling access if so. They also lack an inventive concept, reciting only generic components and functions.

II. LEGAL STANDARD

Abstract ideas are not patentable. *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208, 216-17 (2014). Courts apply a two-step framework to "distinguish[] patents that claim . . . abstract ideas from those that claim patent-eligible application of those concepts." *Id.* at 217. At **step one**, courts determine whether the claims "are directed to a patent-ineligible concept." *Id.* at 218. This requires "looking at the 'focus' of the claims, their 'character as a whole,'" to determine if they are directed to excluded subject matter. *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (citation omitted). "The inquiry often is whether the claims are directed to 'a specific means or method' for improving technology or whether they are simply directed to an abstract end-result." *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1326 (Fed. Cir. 2017) (citation omitted). A claim that can be performed mentally or analogized to brick-and-mortar concepts likely is directed to an abstract idea. *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011) (finding claim directed to fraud detection for electronic interactions an "unpatentable mental process"); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094 (Fed. Cir. 2016) (finding fraud detection claims "merely implement an old practice in a new environment"). Software claims may be abstract if "[t]hey do not claim a particular way of programming [to accomplish the claimed functionality], but instead merely claim the resulting systems" or if they "are not directed to a specific improvement in the way computers operate." *Apple Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241 (Fed. Cir. 2016).

At **step two**, courts remove the abstract idea from the claim and search the remainder for an "inventive concept sufficient to transform" the abstract idea into a patent-eligible application. *Alice*, 573 U.S. at 221 (citation omitted). There is nothing inventive about implementing an abstract idea using "'well-understood, routine, conventional activit[ies]' previously known to the industry," *id.* at 225 (alteration in original), or limiting the abstract idea to a "particular technological environment," *Bilski v. Kappos*, 561 U.S. 593, 610-11 (2010) (citation omitted).

Patent eligibility under § 101 is a question of law which courts may resolve on a motion to dismiss. *See SAP Am., Inc. v. Investpic, LLC*, 898 F.3d 1161 (Fed. Cir. 2018). "[I]n ruling on a 12(b)(6) motion, a court need not 'accept as true allegations that contradict matters properly subject to judicial notice or by exhibit,' such as the claims and the patent specification." *Yu v. Apple Inc.*, 1 F.4th 1040, 1046 (Fed. Cir. 2021) (citation omitted). Amended pleadings are subject to the same standard of legal sufficiency. *Marucci Sports, L.L.C. v. NCAA*, 751 F.3d 368, 378 (5th Cir. 2014).

III. THE FRAUD REDUCTION PATENTS CLAIM INELIGIBLE SUBJECT MATTER

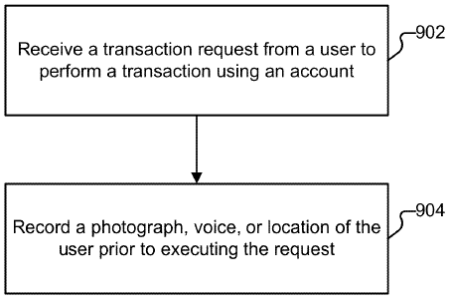
A. Background of the Fraud Reduction Patents and Their Exemplary Claims

The Fraud Reduction Patents—a family that shares the same title, inventor, assignee, and specification—are directed to "[t]echniques for reducing fraud."[2] '010 at Abstract; *see also* Compl. ¶ 54 (alleging these relate to "preventing or reducing fraud in electronic transactions"). These "Fraud Reduction" patents, Compl. ¶ 2, identify a non-technological problem: "Fraudulent transactions are an ongoing problem." '010 at 1:19-29. To address this problem, these patents propose non-technological solutions that increase "the likelihood (either real or . . . perceived . . .) that the fraudulent act will be detected." *Id.* at 4:45-48. To reduce fraud, the patents describe capturing biometrics, such as a fingerprint or photograph, to ensure that the user is authorized to

[2] The Fraud Reduction Patents' specifications are identical other than cross-references to each other. All citations in this section are to the '010 specification.

engage in the transaction. *Id.* at 6:39-45; 8:55-63. Location information can also be captured. *Id.* at 10:10-12. Figure 9, copied below, "illustrates an embodiment of a process for reducing fraud:"

Claim 9 of the '010 is illustrative of the Fraud Reduction Claims and recites:



9: A method, comprising:

receiving a virtual likeness of a face of an account holder;

associating, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;

rendering, in an interface, the virtual likeness of the face of the account holder;

rendering a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;

receiving an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;

capturing contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;

performing a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and

based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information, completing the electronic transaction.

'010, cl. 9.[3] In sum, the claim recites receiving and storing information (a virtual likeness, an

[3] The independent claims of each patent recite substantively similar limitations, respectively reciting either a system, method, or computer readable medium. *Compare* '010, cl. 1, 17 *with* '010 cl. 9; *compare* '656, cl. 1, 19 *with* '656, cl. 10; *compare* '886, cl. 1, 11 *with* '886, cl. 6.

indication of an action, biometric information); displaying information (virtual likeness and icon); analyzing information (a fraud detection analysis); and a result (completing a transaction). The ’656 and ’886 independent claims are similar, except that they also recite capturing location information, and the ’656 recites storing biometric information instead of a virtual likeness. *E.g.*, ’656, cl. 10; ’886, cl. 6. The Fraud Reduction Claims use only functional language directed to the abstract idea of receiving/storing, displaying, and analyzing information, and nothing in this ordered combination of elements provides additional inventive concept to the abstract idea.

Importantly, the claims do not recite ***how*** to perform the purportedly inventive fraud detection analysis. Rather, the claims recite merely an input to that analysis—*i.e.*, biometric (and, for the ’656 and ’886, location) information—and the output of that analysis—*i.e.*, a determination that a user is alive. But the claims are silent on ***how*** anyone would conduct that analysis and do not tether it in any meaningful way to the recited components. As explained below, the specification’s sole reference to detecting “aliveness” is silent on how that process is performed. The fraud detection limitation is directed to a result, rather than a specific means of achieving it.

The asserted dependent claims add minor features that do not change the character of the independent claims. These dependent claims recite merely display of additional information (’010 cls. 5-6, 13-14; ’656 cls. 7-8, 16-17; ’886 cls. 4-5, 9-10); collection of additional information (*e.g.*, user location, audio, photographs) (’010 cls. 21-22; ’886 cls. 4, 9, 14, 20); the origin of collected information (virtual likeness provided by the recipient of a transaction) (’656 cls. 4, 13); information that is not required (a password) (’656 cl. 9, 18); a qualification that the recited transaction involves a payment (’886 cls. 2, 7); and determining whether a face is detected in captured images—without any recitation of how that determination is performed (’886 cls. 12, 18).

During prosecution of the ’010, the examiner rejected the pending claims six times under

§ 101, and applicant overcame these rejections only by adding the step of determining whether a user is "alive." Ex. G ('010 FH) at 8.[4] Later, during prosecution of the '886, the same examiner rejected the pending claims under § 101 even though they recited the "alive" determination, allowing the claims only once the limitation of capturing location data was added. Ex. H ('886 FH) at 15-16, 21-23. As discussed below, neither feature saves the claims from ineligibility.

B. Step One: The Fraud Reduction Patents are Directed to an Abstract Idea

The Fraud Reduction Claims are directed to the abstract idea of collecting, receiving, and analyzing information about a user—namely, biometric (and, for the '656 and '886, location) information—to enable a transaction. The Federal Circuit has held that this is an impermissibly abstract idea. In *USR*, the Federal Circuit affirmed a district court's order granting a motion to dismiss claims directed to the abstract idea of "collect[ing] and examin[ing] data to authenticate the user's identity." 10 F.4th at 1352 (alteration in original). The *USR* claims were directed to the abstract idea of "an electronic ID device that includes a biometric sensor, user interface, communication interface, and processor working together to (1) authenticate the user based on two factors—biometric information and secret information known to the user—and (2) generate encrypted authentication information to send to the secure registry through a point-of-sale device." *Id.* The claims here are even more abstract, directed merely to displaying information, receiving a transaction request from a user, capturing user biometric (and, for the '656 and '886, location) information, and based on the captured information, completing the transaction. *See id.* As in *USR*, the Federal Circuit has held numerous similar claims to be abstract. *E.g.*, *FairWarning*, 839 F.3d at 1093 ("detecting fraud and/or misuse in a computer environment based on analyzing data . . . including user identifier data . . . to determine if the activity indicates improper access" directed to

[4] The court may take judicial notice of file histories in considering a § 101 motion to dismiss. *Data Engine Tech. LLC v. Google LLC*, 906 F.3d 999, 1008 n.2 (Fed. Cir. 2018).

abstract idea); *Elec. Power*, 830 F.3d at 1353 ("collecting information, analyzing it, and displaying certain results of the collection and analysis" directed to abstract idea).

The claims' "essentially result-focused, functional character" confirms that they are "ineligible under § 101." *Elec. Power*, 830 F.3d at 1356. While certain claims recite conventional physical components (*e.g.*, a processor, memory, camera) performing their conventional functions, that is insufficient to render the claims nonabstract. *Yu*, 1 F.4th at 1043 (finding "conventional components [that] perform only their basic functions" simply provide "a generic environment in which to carry out the abstract idea"); *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1168 (Fed. Cir. 2019) ("[T]he physicality of [processing] paper checks" insufficient to salvage abstract idea).

While the Fraud Reduction Claims require that certain information be "captur[ed]" (biometrics, location information) and a certain determination made (whether a user is "alive"), those features do not save the claims from being abstract—for several reasons.

First, collecting and analyzing information is an abstract ineligible idea, and limiting that process to either specific information or a specific technological environment (*e.g.*, an electronic transaction) does not render the claims nonabstract—particularly where the claims, as here, implement the age-old process of capturing and analyzing information about a person before enabling a transaction. *Elec. Power*, 830 F.3d at 1353-54 (claims directed at collecting and analyzing specific data within an electric power grid ineligible); *FairWarning*, 839 F.3d at 1094-95; *Intell. Ventures I LLC v. Erie Indem. Co.*, 850 F.3d 1315, 1330 (Fed. Circ. 2017).

Second, the use of biometric data does not render a claim nonabstract. *USR*, 10 F.4th at 1353. The claims do not purport to improve upon the use of biometrics, describe a new way of performing biometric analyses, or claim new tools for capturing biometrics, and as in *USR*, there "is no description in the patent[s] of a specific technical solution by which the biometric

information . . . is generated." *Id.* at 1352. The claims simply recite using biometric information (*e.g.*, a face) to make a determination—something humans have done for eons. *See, e.g., Blue Spike, LLC v. Google Inc.*, No. 14-cv-01650, 2015 WL 5260506, at *6 (N.D. Cal. Sept. 8, 2015) (steps "mirror[] . . . the human mind"), *aff'd*, 669 F. App'x 575 (Fed. Cir. 2016) (non-precedential).

Third, merely using location information in the '656 and '886 claims does not render them not abstract. The claims provide no new technical solution for capturing or analyzing location information. Using location information only in connection with a transaction is itself an abstract idea. *See, e.g., NEXRF Corp. v. Playtika Ltd.*, 547 F. Supp. 3d 977, 991-92 (D. Nev. 2021) ("incentivizing gambling tailored to a user's location" is abstract), *aff'd*, 2022 WL 1513310 (Fed. Cir. May 13, 2022); *Front Row Techs., LLC v. NBA Media Ventures, LLC*, 204 F. Supp. 3d 1190, 1268, 1273-74 (D.N.M. 2016) (authorizing "video based on a user's location" abstract), *aff'd sub nom. Front Row Techs., LLC v. MLB Adv'd Media, L.P.*, 697 F. App'x 701 (Fed. Cir. 2017) (non-precedential). Verifying location is a longstanding commercial practice and method of organizing human activity. Nevada casinos adopted this practice when they "took steps to ensure that persons seeking to place wagers were" in Nevada. *GeoComply Sols. Inc. v. Xpoint Servs. LLC*, No. 22-1273, 2023 WL 1927393, at *6 (D. Del. Feb. 10, 2023).

Fourth, the claims' recitation of determining whether a user is "alive" does nothing to render the claims nonabstract. *Dropbox, Inc. v. Synchronoss Technologies, Inc.* is particularly instructive. 815 F. App'x 526 (Fed Cir. 2020) (non-precedential). There, the Federal Circuit addressed claims directed to authentication and data security, where the claimed advance over the prior art was a recited "access checker" that permitted access to a resource only if certain specified conditions were met. *Id.* at 533 (affirming district court's dismissal under § 101). The Court found that feature to be only a "functional abstraction" because the specification did not describe a

"technological solution" for its implementation, instead treating the feature "as a black box." The same is true here. The claims here recite nothing more than the end result of determining that the user is alive, without specifying how that is done. The specification contains only a single sentence referencing this feature: "Techniques for confirming that the object being photographed is alive (*e.g.*, by taking multiple photographs in rapid succession) can be employed to help make sure that the fraudster isn't using camera 112 to photograph a printed picture of the legitimate user." 8:55-60. Nowhere does the patent claim or describe ***how*** the photographs are used to determine aliveness, or any other process to determine aliveness. Rather, the patents treat this function as a "black box" "functional abstraction," confirming that the claims are directed to an abstract idea.[5]

The claims are also abstract because they can largely be performed via mental processes. *Blue Spike*, 2015 WL 5260506, at *5. They are analogous to longstanding commercial practices mentally performed by, *e.g.*, bank tellers and notaries. For example, bank tellers assess contextual information (*e.g.*, ID documents, physical appearance, and physical presence) before facilitating a transaction. *See Cybersource*, 654 F.3d at 1373 (identifying fraud based on contextual information "can be performed . . . in the human mind").

Nor do the Fraud Reduction Claims recite any "specific improvement to the way computers operate," *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016), or "overcome a problem specifically arising in the realm of computer networks," *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014). Fraud reduction and consumer

[5] While the '010 and '656 claims recite that aliveness is determined "at least in part" on biometric information, they do not specify the type of biometric information, how it is used, or how the determination is made. As the '886 examiner found, the specification does not disclose using biometrics for checking aliveness. Rather, it discloses checking aliveness only by taking multiple photographs in succession, without specifying what to do with the photographs. *E.g.*, '010, 6:39-45 (biometrics), 8:55-60 (aliveness); '886 FH at 5-6. While the '886 adds that aliveness is determined by analyzing "the set of images," this too is an unexplained black-box determination.

authentication are not unique to electronic transactions, and processes to combat those problems predate electronic commerce. *AuthWallet, LLC v. Block, Inc.*, 602 F. Supp. 3d 620, 635 (S.D.N.Y. 2022) ("Brick-and-mortar retailers who provide for coupons . . . have long faced fraud and verification issues"), *aff'd sub nom. In re AuthWallet, LLC*, No. 2022-1842, 2023 WL 3330298 (Fed. Cir. May 10, 2023). The claims are directed to an abstract idea for these reasons, as well.

C. Step Two: The Fraud Reduction Patents Lack Any Inventive Concept

Once the abstract idea is stripped from the Fraud Reduction Claims, what remains does not add "significantly more" to the abstract idea—certainly nothing "sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 217-18, 221 (citation omitted). All that is left are conventional computer components or components recited in purely functional terms, which is insufficient to transform an abstract idea into a patent-eligible claim. *See id.* at 222-23; *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290-91 (Fed. Cir. 2018) ("If a claim's only 'inventive concept' is the application of an abstract idea using conventional and well-understood techniques, the claim has not been transformed . . . .").

Where the Fraud Reduction Claims recite any hardware at all, that hardware is neither new nor used in any new way, but is instead only conventional, *e.g.*, processors and cameras performing their conventional functions in conventional methods. *E.g.*, '010 at 2:6-10 ("[A] component . . . may be implemented as a general component that is temporarily configured to perform the task"); 3:54-55 ("Telephony device 110 includes typical components such as a CPU, RAM . . . ."). Accordingly, none of the recited hardware components saves the claims from ineligibility. *See, e.g.*, *FairWarning*, 839 F.3d at 1096 ("[U]se of generic computer elements like a microprocessor or user interface do not alone transform an otherwise abstract idea into" a patent-eligible one).

Nor can the routine functions performed by these components, such as "receiving" and "transmitting" information, viewed individually or as an ordered combination, suffice to transform

the claims into a patent-eligible application of the abstract idea. *Affinity Labs v. DirectTV, LLC*, 838 F.3d 1253, 1262 (Fed. Cir. 2016) ("transmitting and receiving signals" is insufficient); *Intell. Ventures I*, 850 F.3d at 1328-29 (sending and receiving information is routine and generic).

Nor are the claims rooted in computer technology to address a problem specifically arising in the realm of computer networks. Rather, they address problems that predate computers and e-commerce. *See Intell. Ventures I*, 850 F.3d at 1327 (concluding claimed activity was abstract as it was "longstanding conduct that existed well before the advent of computers and the Internet"). The emphasis on techniques for fraud reduction, *e.g.*, '010 at 4:41-42, demonstrates that the '010, '656, and '886 merely purport to solve longstanding, non-technical problems.

Moreover, unlike in *DDR Holdings*, 773 F.3d at 1258, none of the claims purport to override the normal operation of the claimed components. *Cf. id.* at 1258 (finding claims patent-eligible where the claims "specif[ied] how interactions with the Internet are manipulated to yield a desired result—a result that overrides the routine and conventional sequence of events ordinarily triggered by the click of a hyperlink"). Capturing biometric information after a transaction request is made, and enabling a transaction after that captured information is analyzed, is entirely normal.

Moreover, the claims here lack the specificity necessary to support an inventive concept. *See Yu*, 1 F.4th at 1045 ("Because claim 1 is recited at a high level of generality and merely invokes well-understood, routine, conventional components to apply the abstract idea" claim 1 fails at step two.). Exemplary '010 claim 9 recites "capturing contextual information" and "performing a fraud detection analysis" by determining "that the user is alive," but provides no specificity on *how* to perform these steps. No algorithms are disclosed, let alone claimed. The only disclosure of determining aliveness states only a functional result: using a typical camera to take conventional photographs, with the goal of distinguishing a live user from a photograph. '010, 8:55-60. The

claims are "directed to a result . . . that itself is the abstract idea and merely invoke[s] generic processes." *USR*, 10 F.4th at 1357 (internal citations omitted).

No detail recited in the '010's dependent claims or the '668 and '886 claims (such as conducting the fraud reduction analysis using location data, voice data, or sets of photographs) changes the analysis, as these limitations are still insufficiently specific. *See id*. (finding claims "insufficiently specific" due to reciting only "conventional" authentication techniques and finding dependent claims' further specificity on "what comprises" the secret information or authentication information still lacking). While the '886 recites a camera to take a set of images as the biometric information, taking photos is the conventional use of a camera, and there is no specificity (let alone inventiveness) in ***how*** the set of images is analyzed to determine aliveness, nor any kind of technological advancement in the camera or process disclosed. *See Yu*, 1 F.4th at 1045.

Finally, there is no inventive concept in the claims' ordered combination of elements. Receiving and then analyzing biometric information before authorizing a transaction is entirely conventional and nowhere does the specification contend that the recited steps provide an unexpected improvement. *See USR*, 10 F.4th at 1358 (concluding that nothing in specification suggested that its combination of conventional techniques results in unexpected improvement). Instead, the Fraud Reduction patents admit the order "may be altered within the scope of the invention." *E.g.*, '010, 2:4-5. In short, "[t]he features set forth in the claims are described and claimed generically rather than with the specificity necessary to show how those components provide a concrete solution to the problem addressed by the patent." *Affinity Labs v. Amazon.com Inc.*, 838 F.3d 1266, 1271 (Fed. Cir. 2016). This is not enough to make the claims patent-eligible.

IV. THE AUTHENTICATION PATENTS CLAIM INELIGIBLE SUBJECT MATTER

A. Background of the Authentication Patents and Their Exemplary Claims

The Authentication Patents purport to improve existing "authentication techniques" by

making accessing resources less "tedious." '138, 3:1-43, 3:61-64. The "Authentication Patents," Compl. ¶ 2, have the same title, inventor, and assignee, and share similar specifications.[6] Their purported solution is to verify the user's identity by matching biometric information (*e.g.*, fingerprint) to a template (*e.g.*, fingerprint patterns) before sending the user's credentials (*e.g.*, passwords) to a requested resource on the user's behalf. '138, 3:1-4. Users thus "need not type . . . usernames and passwords into their devices" ('138, 2:65-3:1), and may instead "authenticate themselves to an 'authentication translator'" that handles the credentials. '138, 3:1-4.

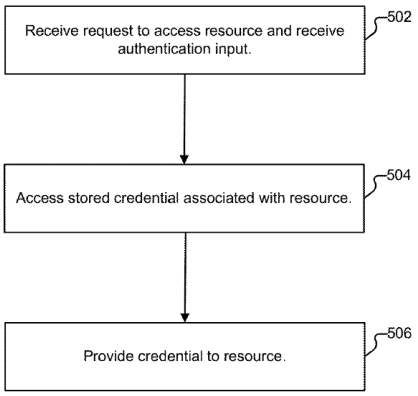
'138 claim 13 is illustrative of the Authentication Patents Claim and recites:

> 13. A method, comprising:
>
> based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate access of at least one record stored at least in part in a storage on the device, wherein the storage on the device is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device;
>
> wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
>
> a biometric template; and
>
> a credential comprising a cryptographic key;
>
> in response to determining a match between a biometric input and the biometric template, retrieving, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
>
> establishing a connection with the external resource;
>
> facilitating a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
>
> facilitating, by the processor on the device, wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part

[6] The '512 and '138 have identical specifications. The '105 specification adds to the '138 specification Figs. 9-15, and an "ADDITIONAL EMBODIMENTS" section. Unless stated otherwise, all citations are to the '138 specification.

in the storage on the device.

'138, cl. 13.[7] Figure 5 of the patents, copied in full below, "illustrates an embodiment of a process for performing authentication translation" (*id.*, Fig. 5):



In sum, the claim recites storing information (a record comprising a biometric template and cryptographic key); displaying information (a prompt); receiving information (a biometric input); analyzing information (determining a match between received and stored information); accessing information (accessing a credential); transmitting information (transmitting the credentials); and removing information (facilitating wiping of information). '138, 3:21-55, 4:44-46, 6:29-7:23, Fig. 5. The independent claims of the '105 and '512 are similar, except neither recites a visual prompt or wiping data, the '105 recites "initiating a backup" to a device (without reciting how) and receiving and matching "authentication information," without specifying how or what, '105, cl. 18; and the '512 recites two processors (instead of one) and performing a backup to a storage service,'512 cl. 11. The Authentication Patent Claims do not recite any new "authentication technique." And they disclose no new technology for performing any claimed function.

Instead, the patents emphasize that their authentication techniques are "widely deployable" by using "general component[s]" and can be implemented "in numerous ways," in a "variety . . .

[7] The independent claims of each patent recite substantively similar limitations respectively reciting either a system, method, or computer readable medium. *Compare* '138, cl. 1, 25 *with* '138 cl. 13; *compare* '105, cl. 1, 35 *with* '105, cl. 18; *compare* '512, cl. 1, 11 *with* '512, cl. 21.

of devices" (including "gaming systems," "mice," and "door locks") in "a variety of places within an environment" to conduct "a variety" of transactions with a "variety of services." '138, 1:44-46, 2:6-23, 2:36-3:16, 4:35-37. The "general component[s]" used to perform the techniques—*e.g.*, generic processors, memory, storage, and "standard commercially available server hardware"—are recited as performing their conventional functions, such as receiving, analyzing, and transmitting data. '138, 2:16-23, 3:60-4:3, 4:13-4:31, 5:10-45, 6:50-57, 7:48-8:2, 9:17-22, Fig. 5.

The dependent claims add minor features that do not change the character of the independent claims. They recite merely backing up and storing information ('138 cls. 10, 12, 22, 24; '105 cls. 9, 28; '512 cls. 2-3, 12-13); wiping information ('138 cls. 7-8); generic encryption/decryption ('512, cls. 4, 10, 14, 20); and otherwise generic components ('138 cls. 11, 23; '105 cl. 11 (restricted interface); '138, cl. 3, 15 (sensor)).

B. Step One: The Authentication Patents are Directed to an Abstract Idea

The Authentication Patent Claims are directed to the idea of facilitating access to resources based on authenticating a user's identity, an idea the Federal Circuit has already held is impermissibly abstract. *E.g.*, *USR*, 10 F.4th at 1346, 1355-58 (holding abstract claims directed to "authenticating a user for enabling a transaction" and explaining "cases involving authentication technology" often turn on *Alice* step 2); *Prism*, 696 F. App'x at 1016 (claims directed to "providing access to resources" impermissibly abstract). Indeed, the claims here are analogous to those the Federal Circuit found ineligible in both *USR* and *Prism*. Here, as in *USR*, the claims are abstract because they "'simply recite conventional actions in a generic way' (*e.g.*, receiving a transaction request, verifying the identity of a customer . . . allowing a transaction) and 'do not purport to improve any underlying technology.'" 10 F.4th at 1349-50 (citation omitted). And in *Prism*, the claims recited "(1) receiving identity data from a device with a request for access to resources;" (2) "confirming the authenticity of the identity data;" "(3) determining whether the device

identified is authorized;" and "(4) if authorized, permitting access." 696 F. App'x at 1017 (finding claims do not "cover a concrete, specific solution to a real-world problem"). The claims here similarly recite storing authentication information; receiving a user's request for access to resources; receiving identity data; determining a match between received and stored authentication information; and, if authorized, accessing and transmitting credentials to permit access.[8]

While some asserted claims recite displaying a prompt to input information and facilitating wiping information, these features do not save these claims from being abstract as these features recite conventional actions in a generic way and "do not purport to improve any underlying technology." *See USR*, 10 F.4th at 1349-50 (citation omitted). The Federal Circuit has found such limitations abstract. *E.g.*, *Elec. Power*, 830 F.3d at 1355 (conventional display technology).

The "essentially result-focused, functional character" of the Authentication Patent Claims confirms they are "ineligible under § 101." *See Elec. Power*, 830 F.3d at 1356. While certain claims recite generic physical components (*e.g.*, interface, processor, storage, camera) performing their standard functions, that is insufficient to render the claims nonabstract as a matter of law. *See Yu*, 1 F.4th at 1043; *Solutran*, 931 F.3d at 1168.

Instead of being "necessarily rooted in computer technology . . . to overcome a problem specifically arising in the realm of computer networks," *DDR Holdings*, 773 F.3d at 1265, the claims merely introduce existing practices and mental processes into a new technological environment—a hallmark of ineligibility. *E.g.*, *FairWarning*, 839 F.3d at 1094-95 (invalidating claims that "merely implement an old practice in a new environment"); *Intell.Ventures I*, 850 F.3d

[8] That these steps can be performed mentally or with pen and paper further underscores their abstractness. *See, e.g.*, *CyberSource*, 654 F.3d at 1371 ("[M]ethods which can be performed mentally . . . are unpatentable abstract ideas."). Facilitating access to a resource based on authenticating someone's identity requires nothing more than one's mind.

at 1330 (similar); *Umbanet, Inc. v. Epsilon Data Mgmt., LLC*, 263 F. Supp. 3d 647, 653 (E.D. Tex. 2017) (finding claims limited to a specific technological environment abstract where the "underlying concept . . . is abstract"), *aff'd*, 745 F. App'x 168 (Fed. Cir. 2018) (non-precedential). Facilitating access to a resource after authenticating a person's identity is an activity that humans have long performed. For example, security guards have long been stationed at a building's entrance to verify a visitor's identity before allowing access, and to advise a building occupant of the visitor's arrival. Commonly, security guards require a photo ID, copy IDs for future verification, and provide access passes so authorized visitor can proceed unimpeded, and wipe personal records (*e.g.*, copies of IDs) when they are outdated or not needed. *Prism*, 696 F. App'x at 1017 (brief notes "pre-computer-age corollaries") (citing Ex. I (Brief) at 58-59 (describing security guard ID check)). Other limitations do not change the nature of the claims' abstract idea.

First, backing up (securely), storing, and wiping information, and generic encryption/decryption, does not render a claim nonabstract. *Elec. Power*, 830 F.3d at 1355-56 ("[T]he essentially result-focused, functional character of claim language has been a frequent feature of claims held ineligible under § 101."). The claims do not purport to improve upon techniques for backing up, storing, or wiping information, or for encryption/decryption; to describe an inventive manner doing so; or to claim inventive tools for doing so. *See Alice*, 573 U.S. at 226. Such limitations are commonly found abstract. *See also WhitServe LLC v. Dropbox, Inc.*, 854 F. App'x 367, 371-72 (Fed. Cir. 2021) (non-precedential) ("maintaining data records, including storing records at different sites for added protection" is abstract); *RecogniCorp*, 855 F.3d at 1327. Moreover, these are things humans have done for decades. *See Blue Spike*, 2015 WL 5260506, at *5. Some claims recite backing up to either a device or a storage, but no claim describes ***how*** to do so and thus cannot render the claims nonabstract. Some claims recite backing up devices of the

same brand, but again does not recite how. "Adding one abstract idea . . . to another . . . does not render the claim nonabstract." *RecogniCorp*, 855 F.3d at 1327.

Second, generic computer components (*e.g.*, sensors, secure storage, processors) cannot render the claims not abstract. *Alice*, 573 U.S. at 226.

Third, for the same reasons that mere use of biometric information does not render a claim nonabstract, mere use of "authentication information" does not render a claim nonabstract. Rather, the broad scope of "authentication information" described in the specification—*e.g.*, any biometric data, profiles, templates, vaults, credentials, cryptographic keys, or passwords, '105, 4:18-22, 8:47-52, 19:37-42, 20:22-27—supports that the claims are abstract. *See Elec. Commc'n Techs., LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1181-82 (Fed. Cir. 2020) (finding broad scope of "authentication information" in specification supported abstractness).

C. Step Two: The Authentication Patents Lack Any Inventive Concept

Patent eligibility of authentication technology "often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." *USR*, 10 F.4th at 1346. The Authentication Patent Claims fall far short. Once the abstract idea is stripped from the claims, all that is left are generic or conventional components, or components recited in purely functional terms, none of which is sufficient. *See Alice*, 573 U.S. at 222-23.

The hardware recited in the Authentication Patent Claims is generic and conventional. There is nothing inventive about these components themselves, as the specification affirms. '138, 2:16-20 (processor and memory "may be implemented as 'general component[s]'"); 3:66-4:5 (sensor as "*e.g.*, a camera or fingerprint reader"). *See Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324-25 (Fed. Cir. 2016) ("interface" fails to satisfy the inventive concept requirement); *WhitServe LLC.*, 854 F. App'x at 372 ("storing data is a generic computer function"). The biometric limitations are also generic. '138, 3:31-35, 4:38-40 (may be a

fingerprint, photograph, voiceprint, retina scan, typing speed), 3:31-35, 4:38-40 (biometric template may be fingerprint patterns, a photograph).

Likewise, the routine functions performed by these components, such as "receiving," "transmitting," and securely "storing" data, viewed individually and as an ordered combination, do not transform the abstract idea into patent-eligible subject matter. *See, e.g.*, *Intell. Ventures I*, 850 F.3d at 1329 (sending/receiving data using computers is routine and generic); *WhitServe LLC.*, 854 F. App'x at 372 (finding "storing data is a generic computer function" and "[i]t is a well-understood practice of human organization that backup copies are stored in a location separate and distinct from the original," citing bank safe deposit boxes); *Sensormatic Elecs., LLC v. Wyze Labs, Inc.*, 484 F. Supp. 3d 161, 167-69 (D. Del. 2020) ("'securing the storage and transmission of data' . . . are just features of the abstract idea"), *aff'd*, 2021 U.S. App. LEXIS 20789 (Fed. Cir. July 14, 2021).). Nor is distributing operations across two generic processors (*e.g.*, '512, cl. 11) inventive. *See SAP Am.*, 898 F.3d at 1169-70 ("'parallel processing' computing architecture" not an inventive concept); *Coho Licensing LLC v. Glam Media, Inc.*, 2017 WL 6210882, at *6 (N.D. Cal. 2017) ("divide-and-conquer distributive computer processing" claims lack inventive concept) *aff'd sub nom. Coho Licensing LLC v. Oath Inc.*, 710 F. App'x. 892 (Fed. Cir. 2018).

The claims lack the specificity necessary to support an inventive concept. '138, 3:31-35, 4:38-40 ("biometric information"); '105, 4:18-22, 8:47-52, 19:37-42, 20:25-27 ("authentication information"); *Affinity Labs*, 838 F.3d at 1271 ("[F]eatures . . . are described and claimed generically," not "with the specificity necessary to show how those components provide a concrete solution"); *Maxon, LLC v. Funai Corp.*, 726 F. App'x 797, 799-800 (Fed. Cir. 2018) (non-precedential) (non-inventive as patent did not limit the breadth of claim's physical components).

The claims also are not rooted in computer technology to address a problem specifically

arising in the realm of computer networks. The "tedium" of accessing a resource is not specific to computers. '138, 1:35-46. And "merely adding computer functionality to increase the speed . . . does not confer patent eligibility on an otherwise abstract idea." *Intell. Ventures I LLC v. Cap. One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015)). Moreover, the claims do not purport to override the normal operation of the claimed components. *Cf. DDR*, 773 F.3d at 1258.

And there is no inventive concept in the claims' ordered combination of elements. Storing, displaying, receiving, analyzing, and accessing authorization data before transmittal and wiping is entirely conventional and nowhere does the specification contend that the recited steps provide an unexpected improvement. *See USR*, 10 F.4th at 1358. Instead, the patents admit that "the order of steps" "may be altered within the scope of the invention." '138, 2:14-15.

V. NO ADDITIONAL FACT FINDING IS NECESSARY TO DECIDE THIS MOTION

There can be no genuine issue of disputed fact over whether any claim is well-understood, routine, and conventional so as to make this motion premature. *See Yu*, 1 F.4th at 1046 (court need not accept conclusory allegations contradicted by patent); *United States v. St. Luke's Episcopal Hosp.*, 355 F.3d 370, 377 (5th Cir. 2004) (If "an allegation is contradicted by . . . an exhibit . . ., then indeed the exhibit . . . controls."); *Compare supra* §§ III-IV, *with* Compl. ¶¶ 49-50, 61-62. Nor does the claims' patent eligibility turn on any claim construction. *See Fairwarning*, 839 F.3d at 1098 (patent ineligible regardless of resolution of construction issue).

VI. DISMISSAL WITH PREJDUCE WARRANTED

The Court should dismiss the Complaint with prejudice as no asserted claim is subject-matter eligible, and any amendment would be futile as contradicting records that may be judicially noticed—the claims, specifications, and file histories. *See Legate v. Livingston*, 822 F.3d 207, 211 (5th Cir. 2016) ("[A] district court need not grant a futile motion to amend.").

Dated: May 24, 2023

/s/ Melissa R. Smith

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

James Travis Underwood
Texas Bar No. 24102587
GILLAM & SMITH, LLP
102 N. College, Suite 800
Tyler, Texas 75702
Telephone: (903) 934-8450
Facsimile: (903) 934-9257
Email: travis@gillamsmithlaw.com

James R. Batchelder (*pro hac pending*)
Andrew Radsch
James Mack (*admission pending*)
ROPES & GRAY LLP
1900 University Avenue
East Palo Alto, CA 94303-2284
Tel: 650-617-4000
Fax: 650-617-4090
James.Batchelder@ropesgray.com
Andrew.Radsch@ropesgray.com
James.Mack@ropesgay.com

Cassandra Roth (*pro hac vice pending*)
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
Phone: +1-212-596-9000
Fax: +1-212-596-9090
Cassandra.Roth@ropesgray.com

Allen S. Cross (*pro hac vice pending*)
Nicole Pobre (*pro hac vice pending*)
ROPES & GRAY LLP
2099 Pennsylvania Avenue, N.W.
Washington, DC 20006
Telephone: (202) 508-4600

Facsimile: (202) 508-4650
Allen.cross@ropesgray.com
Nicole.Pobre@ropesgray.com

S. Lara Ameri (*pro hac vice pending*)
Ropes & Gray LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
Phone: +1-617-951-7000
Fax: +1-617-951-7050
Lara.Ameri@ropesgray.com

Attorneys for Defendant, Apple Inc.

CERTIFICATE OF SERVICE

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

/s/ Melissa R. Smith
Melissa R. Smith