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

| | |
|---|---|
| **CARBYNE BIOMETRICS, LLC,**<br><br>**Plaintiff,**<br><br>**v.**<br><br>**APPLE INC.,**<br><br>**Defendant.** | **Civil Action No. 1:23-cv-00324-ADA**<br><br>**JURY TRIAL** |

**PLAINTIFF CARBYNE BIOMETRICS, LLC'S RESPONSE TO DEFENDANT APPLE, INC.'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 ..... 1

A. Rule 12(b)(6) Motion to Dismiss ..... 1

B. Patent Eligibility Under 35 U.S.C. § 101 ..... 2

III. ARGUMENT ..... 3

A. Apple Has Not Met Its Burden of Proving the Two Allegedly "Representative Claims" Are Representative of Every Asserted Claim in the Patents. ..... 4

1. The Authentication Patents contain distinct limitations. ..... 5

2. The Fraud Reduction Patents contain distinct limitations. ..... 7

B. The Authentication & Fraud Reduction Patents Claim Eligible Subject Matter ..... 9

1. The Authentication Patents claim eligible subject matter. ..... 9

a) *Alice* Step One: The asserted claims solve computer problems and improve computer capabilities and are not abstract. ..... 9

b) *Alice* Step Two: As alleged in the Complaint, the claims of the Authentication Patents recite inventive concepts. ..... 13

2. The Fraud Reduction Patents claim eligible subject matter. ..... 14

a) *Alice* Step One: The Fraud Reduction Claims solve computer problems and improve computer capabilities and are not abstract. ..... 15

b) *Alice* Step Two: As alleged in the Complaint, the Fraud Reduction Claims recite inventive concepts. ..... 19

IV. CONCLUSION ..... 20

## TABLE OF AUTHORITIES

**Page(s)**

**CASES**

*Aatrix Software, Inc. v. Green Shades Software, Inc.*,
882 F.3d 1121 (Fed. Cir. 2018)..... 2, 4, 13, 20

*Alice Corp. Pty. Ltd. v. CLS Bank Int'l*,
573 U.S. 208 (2014) .....2,3

*Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*,
841 F.3d 1288 (Fed. Cir. 2016).....9, 14

*AML IP, LLC v. ALDI, Inc.*,
No. 6:21-cv-00605-ADA, Dkt. 40 (W.D. Tex. Oct. 20, 2022) (Albright, J.).....2

*Ancora Techs., Inc. v. HTC Am., Inc.*,
908 F.3d 1343 (Fed. Cir. 2018).....3, 9, 16

*BASCOM Glob. Internet Servs. v. AT&T Mobility LLC*,
827 F.3d 1341 (Fed. Cir. 2016).....14, 20

*Bell Atl. Corp. v. Twombly*,
550 U.S. 544 (2007) .....1

*Berkheimer v. HP Inc.*,
881 F.3d 1360 (Fed. Cir. 2018).....3, 5

*Cellspin Soft, Inc. v. Fitbit, Inc.*,
927 F.3d 1306 (Fed. Cir. 2019).....2, 3, 19

*CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*,
15 F.4th 1091 (Fed. Cir. 2021) .....19

*CyberSource Corp. v. Retail Decisions, Inc.*,
654 F.3d 1366 (Fed. Cir. 2011).....17

*Elec. Commc'n Techs., LLC v. ShoppersChoice.com, LLC*,
958 F.3d 1178 (Fed. Cir. 2020).....12

*Enfish, LLC v. Microsoft Corp.*,
822 F.3d 1327 (Fed. Cir. 2016).....3, 11

*FairWarning IP, LLC v. Iatrci Systems, Inc.*,
839 F.3d 1089 (Fed. Cir. 2016).....17

*Grecia Est. Holdings LLC v. Meta Platforms, Inc.*,
605 F. Supp. 3d 905 (W.D. Tex. 2022) (Albright, J.) .....4

*Illumina, Inc. v. Ariosa Diagnostics, Inc.*,
967 F.3d 1319 (Fed. Cir. 2020).....2

*In re Katrina Canal Breaches Litig.*,
495 F.3d 191 (5th Cir. 2007) .....2

*Mytee Prods. v. Harris Rsch., Inc.*,
439 F. App'x 882 (Fed. Cir. 2011).....20

*PPS Data, LLC v. Jack Henry & Assocs., Inc.*,
404 F. Supp. 3d 1021 (E.D. Tex. 2019) .....4, 5

*Prism Techs. LLC v. T-Mobile USA, Inc*,
696 F. App'x 1014 (Fed. Cir. 2017).....11, 12

*SRI Int'l, Inc. v. Cisco Sys., Inc.*,
930 F.3d 1295 (Fed. Cir. 2019).....9, 11, 16

*TecSec, Inc., v. Adobe Inc.*,
978 F.3d 1278 (Fed. Cir. 2020).....passim

*Universal Secure Registry v. Apple, Inc.*,
10 F.4th (Fed. Cir. 2021) .....12, 17

*Visual Memory LLC v. NVIDIA Corp.*,
867 F.3d 1253 (Fed. Cir. 2017).....19

**STATUTES**

35 U.S.C. § 101.....passim

35 U.S.C. § 112.....19

35 U.S.C. § 282.....4

**OTHER AUTHORITIES**

Fed. R. Civ. P. 12(b) .....1, 2, 3

## TABLE OF ABBREVIATIONS

| TERM | DEFINITION |
|---|---|
| Carbyne | Plaintiff Carbyne Biometrics, LLC |
| Apple | Defendant Apple, Inc. |
| ’512 Patent | U.S. Patent No. 10,929,512 (Dkt. 1-1) |
| ’105 Patent | U.S. Patent No. 11,475,105 (Dkt. 1-2) |
| ’138 Patent | U.S. Patent No. 11,514,138 (Dkt. 1-3) |
| ’010 Patent | U.S. Patent No. 9,972,010 (Dkt. 1-4) |
| ’656 Patent | U.S. Patent No. 10,713,656 (Dkt. 1-5) |
| ’886 Patent | U.S. Patent No. 11,526,886 (Dkt. 1-6) |
| Asserted Patents | ’512, ’105, ’138, ’010, ’656, and ’886 Patents |
| Authentication Patents | ’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 |
| Fraud Reduction Patents | ’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 |
| Asserted Claims | Authentication Claims and Fraud Reduction Claims |
| Motion or Mot. | Apple’s Motion to Dismiss (Dkt. 14) |

## TABLE OF EXHIBITS

| EXHIBIT | DESCRIPTION |
|---|---|
| 1 | *Samsung Electronics Co., LTD. et al v. RightQuestion, LLC,* IPR2022-00251, Paper 17 (PTAB Jun. 09, 2022) (Final Written Decision denying institution) |

## I. INTRODUCTION

Apple's Motion to Dismiss should be denied for several independent reasons. ***First***, Apple has provided no meaningful analysis to support conflating the sixty-three Asserted Claims across the six Asserted Patents into two allegedly representative claims. The six Asserted Patents fall into two technology areas: the '512, '105, and '138 Patents are the "Authentication Patents" and the '010, '656, and '886 Patents are the "Fraud Reduction Patents." With no basis or analysis, Apple asserts that claim 13 of the '138 Patent is representative of the thirty-one asserted claims of the three Authentication Patents and claim 9 of the '010 Patent is representative of the thirty-two asserted claims of the three Fraud Reduction Patents. There is no agreement on representativeness, Apple has not shown its proposed claims are representative, and the Asserted Claims have substantial differences. ***Second***, Carbyne's well-pleaded allegations establish that the claims of the Asserted Patents recite unconventional improvements to user-authentication and computer fraud-reduction technologies. Apple's *Alice* step one arguments rely on reducing the claims of the Asserted Patents to a level of abstraction that is divorced from the claim language—exactly what the Supreme Court and the Federal Circuit instruct against. ***Third***, while this Court need not reach step two of the *Alice* test, Apple's arguments there fail as well because they amount only to unsubstantiated attorney arguments which, at most, suggest factual and claim-construction disputes. Thus, Apple's Motion should be denied.

## II. LEGAL STANDARD

### A. Rule 12(b)(6) Motion to Dismiss

Dismissal at the pleading stage is improper if a complaint alleges "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). When deciding a Rule 12(b)(6) motion to dismiss for failure to state a claim, the court "accepts all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff."

*In re Katrina Canal Breaches Litig.*, 495 F.3d 191, 205 (5th Cir. 2007) (citations omitted).

Patent eligibility can be determined on a motion to dismiss "only 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). For example, a factual dispute over "[w]hether the claim elements or the claimed combination are well-understood, routine, [or] conventional" will preclude granting a motion to dismiss. *Id.* at 1128. And because patents are presumed valid, "[a]ny fact . . . pertinent to the invalidity conclusion must be proven by clear and convincing evidence." *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019). Indeed, this Court has held that a Rule 12(b) motion is an "awkward place" to determine § 101 eligibility:

> In other words, to prevail, the movant needs to overcome both a factual deck stacked against it and a heightened burden of proof. Therefore, because a patent is presumed valid and requires clear and convincing evidence to prove its invalidity, a Rule 12(b) motion to dismiss is a procedurally awkward place for a court to resolve a patent's § 101 eligibility.

*AML IP, LLC v. ALDI, Inc.*, No. 6:21-cv-605-ADA, Dkt. 40 at 7 (W.D. Tex. Oct. 20, 2022).

**B. Patent Eligibility Under 35 U.S.C. § 101**

Whether a patent recites patent-eligible subject matter under § 101 involves a two-step analysis according to the test set forth in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014). Apple, as the party challenging the validity of the Asserted Patents, bears the burden of proof. *Illumina, Inc. v. Ariosa Diagnostics, Inc.*, 967 F.3d 1319, 1328 (Fed. Cir. 2020).

***Alice Step One***. At step one, the court determines "whether the claims at issue are directed to a patent-ineligible concept," like an abstract idea. *Alice*, 573 U.S. at 218. To make this determination, courts ask "what the patent asserts to be the focus of the claimed advance over the prior art" by considering the asserted claims "in light of the specification." *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1292 (Fed. Cir. 2020). In cases involving inventions related to

computer technology, the Federal Circuit has found that claims are patent eligible when they focus on: (1) "specific asserted improvements in computer capabilities," or (2) "a solution to a problem specifically arising in the realm of computer networks or computers." *Id. at* 1293. Notably, the Federal Circuit has held that "[i]mproving security . . . 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." *Id.* at 1294 (quoting *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018)). At step one, courts must avoid describing the claims at "a high level of abstraction" or "untethered from the language of the claims" because doing so "all but ensures that the exceptions to § 101 swallow the rule." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016).

***Alice Step Two***. If a patent claim fails at step one, the court proceeds to step two where it "examine[s] the elements of the claim to determine whether it contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (citations and quotations omitted). Patent claims recite an "inventive concept" if they reflect "something more than well-understood, routine, conventional activities previously known to the industry." *Cellspin*, 927 F.3d at 1315 (citation omitted). "[W]hether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact" that "must be proven by clear and convincing evidence." *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). For a Rule 12(b) motion, Carbyne need only assert "plausible and specific factual allegations that aspects of the claims are inventive." *Cellspin*, 927 F.3d at 1317.

## III. ARGUMENT

The relevant question at the motion to dismiss stage is whether Carbyne has stated a legally plausible claim; not whether it will ultimately be entitled to relief. *See supra* Section II.A.

Carbyne's factual allegations must be taken as true, with every inference made in Carbyne's favor. *Id.* In the Complaint, Carbyne adequately alleged that Apple infringes its duly issued patents and that each Asserted Patent is directed to patent-eligible subject matter and claims unconventional, inventive concepts. Carbyne has thus adequately pled legally sufficient claims, and dismissal at this early stage of the case is inappropriate. *Aatrix Software*, 882 F.3d at 1128.

### A. Apple Has Not Met Its Burden of Proving the Two Allegedly "Representative Claims" Are Representative of Every Asserted Claim in the Patents.

Apple argues that the six Asserted Patents should be held invalid and the entire case dismissed based on a ***completely*** unsupported assertion that two claims—claim 13 of the '138 Patent (Authentication Patents) and claim 9 of the '010 Patent (Fraud Reduction Patents)—are representative of the sixty-three Asserted Claims of the Asserted Patents. Apple's argument fails.

According to 35 U.S.C. § 282, "[e]ach claim of a patent (whether in independent, dependent, or multiple dependent form) shall be presumed valid independently of the validity of other claims." "Absent a basis to overcome the presumption of independence, the plain text of § 282 requires courts to analyze the validity of each claim individually." *PPS Data, LLC v. Jack Henry & Assocs., Inc.*, 404 F. Supp. 3d 1021, 1030 (E.D. Tex. 2019); *Grecia Est. Holdings LLC v. Meta Platforms, Inc.*, 605 F. Supp. 3d 905, 912 (W.D. Tex. 2022) (Albright, J.) ("35 U.S.C. § 282 accords a presumption of validity to each patent claim.").

As the movant and proponent of the alleged representativeness, Apple has the burden to overcome the presumption of independent validity of each claim by "offering a substantial rationale for treating a claim as representative of other asserted claims" that is "directly tethered to the claim language." *PPS Data, LLC*, 404 F. Supp. 3d at 1030. In other words, to justify treating one claim from each of the Authentication and Fraud Reduction Patents as representative of all the other Asserted Claims, Apple "must conduct an analysis tethered to the claim language,

to show that there are ***no legally relevant distinctions between the claim identified as representative and the remaining asserted claims***." *Id.* at 1031 (emphasis added). The Federal Circuit has held the presumption of independent validity can be overcome and a claim may be treated as representative only when: (1) "the patentee does not present any meaningful argument for the distinctive significance of any claim limitations not found in the representative claim" or (2) "the parties agree to treat a claim as representative." *Berkheimer*, 881 F.3d at 1365.

Here, Apple has failed to establish that representative treatment is justified. First, the parties have not agreed that the two claims Apple has identified are representative of all the Asserted Claims. Second, Apple has also failed to show that there are no legally relevant distinctions between its representative claims and the remaining claims. As explained below, both the independent and dependent claims of the Fraud Reduction and Authentication Patents include distinct limitations not present in the allegedly representative claims that Apple has overlooked or ignored. Because Apple has failed to meet its burden of proving the two claims it identified are representative of all the Asserted Claims, the Court should deny Apple's Motion.

**1. The Authentication Patents contain distinct limitations.**

In a single footnote, Apple concludes that the '138 Patent's independent claims are substantially similar to (and thus representative of) the claims of the '138, '512, and '105 Patents. Mot. at 14 n.7. Based entirely on this footnote statement, Apple treats claim 13 of the '138 Patent as representative of all thirty-one asserted claims of the Authentication Patents and only applies the *Alice* test to this allegedly representative claim. But there are substantial differences that preclude finding that this single claim is representative.

For example, claim 1 of the '512 Patent discloses a hardware architecture with a "first" and "second processor" wherein each processor is capable of performing explicit tasks. *See, e.g.*, '512 Patent at cl. 1. Further, there are other distinct components in the claims such as "secure"

and "insecure storage" as well as a "restricted interface" for communication between the "first" and "second" processor that are different from the scope of claim 13 of the '138 Patent. *Id*. And these are differences between the alleged representative claim and just one claim of the '512 Patent. Other claims of the '512 Patent add other distinct differences that need to be considered in the § 101 analysis, such as: cloud storage (claim 2); how the encrypted record is downloaded by the second device (claim 4); and how the record is decrypted and stored (claims 5-9). None of this is captured by a single claim from the '138 Patent.

The same is true for the other Authentication Patents. For example, independent claim 1 of the '105 Patent explicitly requires a "first" and "second" device of the "same brand" capable of initiating a backup of a record. None of these limitations are found in claim 13 of the '138 Patent. However, this is just one of the many differences as claim 4 adds a "secure channel" between the first and second devices of the same brand, claim 9 adds a secure storage and the restricted interface, and claims 10 and 11 add limitations to the restricted interface such as it being a dedicated physical connection and/or an application programming interface, respectively.

Notably, the alleged representative claim of the '138 Patent does not even capture all the distinct elements of the claims of the '138 Patent. Consider claims 11 and 12, which claim the hardware system of claim 1 and additionally a "restricted interface" and "secure storage," respectively. Neither of these distinct hardware elements is captured by the alleged representative claim. Accordingly, Apple cannot show that claim 13 is representative of the '138 Patent's claims—let alone all claims of the Authentication Patents. Apple's Motion ignores the distinctions between the Authentication Patents in favor of analyzing a single claim that it alleges is representative, despite meaningful arguments to the contrary. This Court should not treat a single claim in the '138 Patent as representative, and should deny the Motion on this basis.

**2. The Fraud Reduction Patents contain distinct limitations.**

Apple's Motion states in a footnote that the '010, '656, and '886 Patents are "substantively similar." Mot. at 4 n.3. Based entirely on this footnote statement, Apple treats claim 9 of the '010 Patent as representative of all thirty-two Fraud Reduction Claims and analyzes the patent eligibility of only this single "representative" claim under the *Alice* test. *See* Mot. at 6–12. Based entirely on the footnote statement, and as with the Authentication Patents, Apple's "reasoning" does not meet its burden to rebut the presumption of independent validity.

As Carbyne pointed out in its Complaint, the independent claims of the '656 Patent (claims 1, 10, 19) and the '886 Patent (claims 1, 6, 11) include additional limitations that provide technical improvements distinct from the '010 Patent's claims. *See* Compl. ¶¶ 58-59. The method recited in claim 9 of the '010 Patent describes using "captured biometric information" only to determine that the user is alive. All of the '656 Patent's asserted claims add the limitation of comparing this captured biometric information to distinct "***stored*** biometric information" to confirm a user's identity for the purpose of detecting fraud. *E.g.*, Dkt. 1-5 ('656 Patent) at cls. 1, 10, and 19 (emphasis added). Likewise, the '886 Patent's asserted claims add the requirement that the biometric information used to determine whether a user is "alive" must consist of a "set of images" captured using a camera. *E.g.*, Dkt. 1-6 ('886 Patent) at cls. 1, 6, 11. Just as a biometric comparison improves fraud detection through verification, analyzing real-world photos helps to more accurately verify that a party to a remote transaction is alive. Carbyne pointed out both of these advances in the Complaint, meaning it has already provided meaningful arguments for how the '886 and '656 Patents' claims differ from those of the '010 Patent.

Apple's own Motion acknowledges the meaningful distinctions between the independent claims of the '656 and '886 Patents and claim 9 of the '010 Patent:

> [The '010 Patent's . . . claim 9] recites receiving and storing information[];

> displaying information[]; analyzing information[]; and a result[]. The '656 and '886 independent claims . . . ***also*** recite capturing location information, and the '656 recites storing biometric information ***instead*** of a virtual likeness.

Mot. at 4–5 (emphasis added) (citations omitted). Thus, by Apple's own summary, the '656 and '886 Patents' independent claims possess additional limitations over the '010 Patent's claim 9. In fact, the '656 Patent's independent claims include different subject matter altogether. Apple does not bother to explain how these additional limitations are not legally significant. Therefore, Apple has not met its burden of proving that claim 9 of the '010 Patent is representative.

The dependent claims also include limitations beyond those of Apple's proposed representative claim, such as: the '010 Patent's claim 21, wherein collected biometric information comprises a plurality of photographs that are analyzed to determine whether the user is alive; the '656 Patent's claim 18, which recites initiating a transaction without the user needing to input a password (a convenience feature); and the '886 Patent's claim 10, which recites associating the patented interface with a phone, tablet, or laptop, providing for brand or vendor association. Apple downplays these limitations solely with attorney argument, stating that the dependent claims "add minor features that do no change the character of the independent claims." Mot. at 5. But to reach this conclusion, Apple did not analyze the language of the claims. Instead, Apple sorted the dependent claims into generic, arbitrary categories, that its attorneys characterize as "add[ing] minor features," such as "collection of additional information," "origin of collected information," and "information that is not required." *Id.* This sort of analysis, completely untethered from the claim language, and with nothing more than the suppositions of Apple's attorneys, cannot rebut the presumption of independent validity. Thus, Apple has not met its burden of proving that claim 9 of the '010 Patent is representative of the other Fraud Reduction Claims, and its Motion should therefore be denied.

### B. The Authentication & Fraud Reduction Patents Claim Eligible Subject Matter.

#### 1. The Authentication Patents claim eligible subject matter.

The Authentication Patents are directed to specific improvements in computer security, such as using a dedicated processor only accessible over a restricted interface to control access to records stored in secure storage, and not simply "facilitating access to resources based on authenticating a user's identity" as Apple generically suggests. Mot. at 15. In fact, as demonstrated in the following sections, the Authentication Patents are so clearly not directed to an abstract idea, that even Samsung, a party just as sophisticated as Apple, did not raise § 101 as a defense in a litigation two years ago with some of the same patents.[1]

##### a) *Alice* Step One: The Authentication Claims solve computer problems and improve computer capabilities and are not abstract.

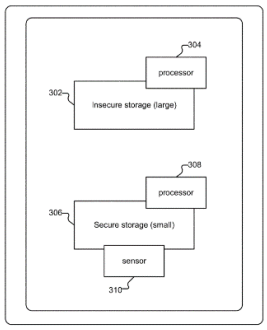
The Authentication Patents provide technical solutions—such as using a dedicated processor only accessible over a restricted interface to limit access to a user's most vital records (their passwords and biometric info)—that overcome issues in the prior art authentication systems to enable safer and more convenient authentication. Separating cryptographic functionality into a specialized secure processor and storage that is difficult to penetrate is a technological solution to a technological problem and not merely the application of an abstract idea using conventional computer technology. *See Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1300 (Fed. Cir. 2016); *Ancora Techs.*, 908 F.3d at 1350 (Claims "yield[ed] a tangible technological benefit (by making the claimed system less susceptible to hacking)."); *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019) (Claims were "directed to using a specific technique . . . to solve a technological problem arising in computer networks:

[1] In fact, the USPTO did not institute IPRs on the '512 Patent, which further demonstrates the inventive concepts of the Authentication Patents. *See* generally Ex. 1.

identifying hackers or potential intruders into the network.”).

The idea to bifurcate the processers and use other means to restrict access to the user’s most vital information is described in the Complaint and specification of the Authentication Patents. For example:

> One example of a device with secure storage is illustrated in FIG. 3. In the example shown, a mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader). Users (and applications) can read from and write to the insecure storage area. However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API.




300 FIG. 3

Dkt. 1-1 (’512 Patent) at 3:66-4:8; Compl. ¶¶ 44-45. As the figure and the description explain, bifurcating the tasks which a first processor and a dedicated second processor are configured to do restricts the first processor from accessing the user’s most vital information which is stored in secure storage and only accessible by the dedicated second processor. *See, e.g.*, Compl. ¶ 32 (“Dr. Jakobsson determined that the correct way to deal with this was to create a secure portion of a device where at least some processing of the user’s most sensitive data would be done.”).

This separation and bifurcation of tasks between processors is also reflected in the claims of the Authentication Patents—but not in the single allegedly representative claim that Apple has elected to focus on. Consider claim 1 of the ’512 Patent, which illustrates this secure division in a system with a “first” and “second” processor where these processors are only capable of communicating with each other via a “restricted interface.” Here, the “first” processor is configured to “establish a secure connection with the external resource,” while the “second” processor is configured to perform many sensitive tasks like “determin[e] that there is a match between the biometric input and a stored biometric template,” “access a record stored in a secure

storage," and "perform a cryptographic operation." Dkt. 1-1 ('512 Patent) at cl. 1; *see also* Dkt. 1-2 ('105 Patent) at cls. 1, 9-11 (discussing different forms of the "restricted interface" such as a "dedicated physical connection" and "application programming interface" to help restrict access to the user's most important information); Dkt. 1-3 ('138 Patent) at cls. 11-12, 23-24.

Indeed, performing these functions on a conventional computer (i.e., that fails to restrict access to a user's most important data) would substantially decrease the security of the overall system, and thus the claimed systems improve the operation of the computer itself. *See Enfish*, 822 F.3d at 1336; *TecSec*, 978 F.3d at 1295. Indeed, the entire point of using a first and second processor—with dedicated tasks that can only communicate with each other in restricted ways—is *not* to use generic computer hardware for the implementation, but rather to use the claimed special-purpose system to improve security. As in *SRI*, the system "improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security." *SRI Int'l, Inc.*, 930 F.3d at 1304.

Apple's arguments to the contrary miss the mark. First, as discussed throughout this brief, Apple's arguments abstract the Authentication Patents beyond comprehension and completely lose sight of the purpose and benefits of their asserted claims and actual disclosures. By describing the Authentication Patents as just "facilitating access to resources based on authenticating a user's identity," Apple abstracts away all of the technical details previously discussed and that are essential to whether the Authentication Patents are eligible under § 101. *See* Mot. at 1. This is exactly what the Federal Circuit warns against. *TecSec*, 978 F.3d at 1295 ("To disregard those express claim elements is to proceed at a high level of abstraction that is untethered from the claim language and that overgeneraliz[es] the claim.") (citations omitted).

Second, after abstracting away all of the technical advances and solutions to problems in

the prior art authentication systems, Apple then tries to analogize its genericized version of the claims of the Authentication Patents to the claims held ineligible in *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1016 (Fed. Cir. 2017) and *Universal Secure Registry v. Apple Inc.*, 10 F.4th 1342, 1346, 1355-58 (Fed. Cir. 2021) ("*USR*"). Mot. at 1-2. Yet, the claims found ineligible in *Prism* and *USR* differ in material ways from the claims of the Authentication Patents. For example, while the claims of the Authentication Patents claim specific hardware implementations that differ from the prior art and solve security issues within authentication systems, that is not the case for the claims in *Prism* and *USR*. In fact, the claims in *Prism* are so basic, that the Federal Circuit found it apt to compare them to "pre-computer-age corollaries for which humans similarly restrict and provide access to resources." *Prism*, 696 F. App'x at 1017. The same is true for the claims in *USR*. *USR*, 10 F.4th at 1349-1350 (discussing how the claims do not depart from earlier approaches to authentication transactions). This is simply not the case with the Authentication Patents. As alleged in the Complaint, the bifurcated use of multiple processors to do distinct tasks to restrict access to a user's most sensitive information solved issues in computing that led users to compromise their own security. *See* Compl. ¶¶ 40-45.

The rest of Apple's arguments are similarly unconvincing. Apple argues that the claims just recite generic computer components. As previously discussed, the entire idea of the claimed bifurcated use of processors and other means to restrict access to users' most sensitive information is the exact opposite of the generic computing approach. Finally, Apple cites to *Elec. Commc'n Techs., LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1181-82 (Fed. Cir. 2020), to argue that the use of "authentication information" in the specification suggests that the claims are abstract. Yet again, Apple's reliance is misplaced. In *Electronic*, "authentication information" was simply "***any*** information recognizable to [a] party." *Id.* at 1181-82 (emphasis

added). Here, by Apple's own admission, "authentication information" is a much narrower subset such as "biometric data, profiles, templates, vaults, credentials, cryptographic keys, or passwords" (Mot. at 18), and not simply "any information recognizable to a party."

**b) *Alice* Step Two: As alleged in the Complaint, the claims of the Authentication Patents recite inventive concepts.**

Even if the Authentication Patents are directed to an abstract idea (which they are not), the claims recite inventive concepts. In its Complaint, Carbyne alleged that the claims of the Authentication Patents, read in light of the specification, "are drawn to solving specific, technical problems arising in authentication systems/methods and provide for advancements in the field that were not routine, well-understood or conventional. Accordingly, the claims of the Authentication Patents recite a combination of elements sufficient to ensure that the claims in practice amount to significantly more than a patent claiming an abstract concept." Compl. ¶ 49; *see also Aatrix Software*, 882 F.3d at 1128.

As alleged in the Complaint, "previous authentication techniques made [p]roviding credentials to a service, whether via a mobile or other device . . . a tedious experience for a user." Compl. ¶ 40 (citations omitted). Further, "[b]ecause the experience was so tedious, users would often engage in practices such as password re-use, and/or the selection of poor-quality passwords, which render their credentials less secure against attacks." *Id.* (citations omitted). The Authentication Patents provide solutions to these exact problems, and the Complaint provides pages of examples regarding how these patents were not well-understood, routine, or conventional improvements to the prior art. *Id.* ¶¶ 40-50.

For example, the Complaint explains that prior art systems contained no notion of using a system with multiple processors and bifurcated tasks to restrict access to the user's most important data stored in secure storage. *Id.* ¶ 44. Thus, this architecture and the protections put in

place by restricting what can access the user's most sensitive data, dramatically improves the authentication experience for users. *Id.* ¶¶ 42-45. In fact, this is just one of several inventive concepts alleged by Carbyne related to the Authentication Patents. *See, e.g.*, *Id.* ¶¶ 47-49 (discussing how "the secure backup," "same brand backup" and "using a cryptographic key as the credential" further enhance the claimed systems). Finally, these inventive concepts are yet again reflected in the claims. *See id.* ¶ 49.

The specification and Carbyne's well-pleaded allegations demonstrate that the claims of the Authentication Patents claim an inventive concept. Yet, *Apple completely ignores these allegations in its Motion*, and offers nothing more than misplaced and conclusory attorney argument to the contrary. Looking at *a single claim* of the Authentication Patents, Apple suggests that using conventional computer components or well-understood techniques means that the Authentication Patents cannot contain an inventive concept. Mot. at 18-19. Not so. The Federal Circuit has repeatedly recognized the patentability of claims despite their recitation of well-known components. *E.g.*, *BASCOM Glob. Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349-50 (Fed. Cir. 2016); *Amdocs*, 841 F.3d at 1300-01. Regardless, without claim construction and guidance from the Court as to the scope of the claims, it is not clear that claim elements like the "restricted interface" and "secure backup" are generic, well-known components as Apple suggests. Mot. at 18 (discussing "interface"). This is especially true here, given that the prior art identified by Samsung in its IPRs did not disclose the alleged generic "restricted interface" among other things. Ex. 1 at 23-26. Such claim construction issues preclude a finding of invalidity at this stage. *AML IP*, No. 6:21-cv-605-ADA, Dkt. 40 at 14-15.

**2. The Fraud Reduction Patents claim eligible subject matter.**

Apple has failed to meet its burden of proving that claim 9 of the '010 Patent (and all other asserted claims) is directed to an abstract idea and does not include an inventive concept.

**a) *Alice* Step One: The Fraud Reduction Claims solve computer problems and improve computer capabilities and are not abstract.**

At *Alice* step one, the relevant questions are whether the claims are directed to (1) "specific asserted improvements in computer capabilities," or (2) "a solution to a problem specifically arising in the realm of computer networks or computers." *TecSec*, 978 F.3d at 1293. The Fraud Reduction Patents meet these requirements.

The Fraud Reduction Claims solve a technological problem specific to computers and computer networks—fraud in electronic payment transactions. As the world economy has increasingly moved online, the transition to the digital commercial environment has created new and unique problems for preventing fraud. Unlike in the past, in the modern digital environment, a fraudster does not need physical access to a victim's credit card or other resources to perpetrate the fraud. Dkt. 1-4 ('010) Patent at 1:24-27. The fraud can be committed remotely by an individual, or even a computer program—anywhere in the world, at any time. Removing the need for a physical link to the victim has made preventing fraud more daunting, as evidenced by the initial prevention techniques that were vulnerable to simple workarounds—like early photo-verification methods that were easily defeated using two-dimensional photos of a legitimate user. *Id.* at 8:58-8:60.

The Fraud Reduction Claims provide a technological improvement over prior authentication techniques for electronic payment transactions by enabling an electronic device to capture and analyze a user's biometric information to determine that the user is alive. As one example, the claims provide for determining a user's "aliveness" by taking multiple photographs of the user in rapid succession to ensure that a fraudster is not simply presenting a printed photo of the legitimate user, thus overcoming the flaw in the earlier photo-verification techniques noted above. *See* '010 Patent at cl. 21 and 8:58-8:60; '886 Patent at cls. 1, 6, 11, 14, and 20. Other rules

can be applied for making this determination and authenticating an electronic transaction, such as, in the photo-verification context for instance, requiring that a face be detected in the captured photo or that the proper amount of flesh tone be present in the picture. '010 Patent at 8:60-8:63.

The Federal Circuit has found patent claims directed to specific authentication or verification methods that depart from previous approaches and improve computer technology—like the claims here—to be eligible under § 101. For instance, in *Ancora*, the Federal Circuit held that claims directed to storing a verification structure in a computer memory were directed to non-abstract improvements in computer functionality by addressing the "vulnerability of license-authorization software to hacking." *Ancora Techs.*, 908 F.3d at 1348-49. As the Federal Circuit explained, these claims "yield[ed] a tangible technological benefit (by making the claimed system less susceptible to hacking)." *Id.* at 1350. Likewise, in *SRI*, the Federal Circuit found claims patent eligible that were "directed to using 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." 930 F.3d at 1303. Like the claims in *SRI* and *Ancora*, the claims here are directed to a specific technique—using biometric data to determine that a user is "alive"—that departs from previous approaches to solve a computer-specific, technological problem—authenticating a transaction over an electronic payment network.

Apple argues that the Fraud Reduction Claims are ineligible under § 101 because: (1) the claims are directed to the abstract idea of "collecting, receiving, and analyzing information about a user to enable a transaction," Mot. at 1, 6; (2) the claims do not recite a specific improvement in the way computers operate or solve a problem specific to computer networks, Mot. at 9-10; and (3) limiting the process of "collection and analysis" to a specific technological environment

(an electronic transaction) and requiring "certain information be captured" (biometrics) and a "certain determination made" (whether the user is alive) do not render the claims nonabstract, Mot. at 7-9. Apple grossly over-genericizes the claims and its arguments fail.

*First*, Apple commits the cardinal sin that the Supreme Court has warned against in § 101 analysis: it oversimplifies the claims at issue. By diminishing the Fraud Reduction Claims to "collecting, receiving, and analyzing information," Apple reads the innovative "aliveness" determination out of the claims, ignores the technical backdrop in which the Fraud Reduction Patents were conceived, and disregards how the "aliveness" determination improves authentication and security in electronic transactions—specifically by improving the technical functionality of the end user's electronic device. *See* '010, '656, and '886 Patents at cl. 1 (claiming a processor equipped with improved biometric authentication capabilities).

The cases Apple cites to support its oversimplified reading of the claims are inapplicable as they do not involve claims that include a technological improvement. In *USR*, the court found that claims reciting the conventional collection and examination of biometric data to authenticate a user's identity were directed to an abstract idea. *USR*, 10 F.4th at 1352. But here, the Fraud Reduction Patents recite a specific technological improvement to the *biometric analysis itself*—the "aliveness" determination—that was missing in the conventional claims the *USR* court found ineligible. Likewise, in *FairWarning IP, LLC v. Iatric Systems, Inc.*, the claims were directed to "the broad concept of monitoring audit log data" and not a problem "specifically arising in the realm of computer technology." 839 F.3d 1089, 1097 (Fed. Cir. 2016) (citations omitted). And in *CyberSource Corp. v. Retail Decisions, Inc.*, the claims were directed to detecting credit card fraud by "utiliz[ing] information relating credit card transactions to particular Internet address[es]"—which is not a computer-based problem. 654 F.3d 1366, 1368 (Fed. Cir. 2011).

*Second*, Apple's contention that the claims are not directed to a computer-specific problem and can be performed using mental processes is simply incorrect. As already explained, the Fraud Reduction Claims provide a specific solution to unique problems posed by authenticating a transaction in a remote digital environment. *Supra*, at 9-10. The claims are also not like the commercial tasks performed by bank tellers and notaries, as Apple suggests, because the need for the claimed "aliveness" determination arises only in the unique context of a digital environment where a person's physical presence is not required to complete a transaction—thus confirming the Fraud Reduction Claims address a problem specific to computer technology.

*Finally*, Apple's third argument falls flat. In making this argument, Apple undermines its core argument—that the Fraud Reduction Claims are abstract and lack specificity—by pointing out that the claims require capturing "*certain*" information and making a "*certain*" determination. Mot. at 7. Besides this obvious contradiction, Apple's specific points supporting its third argument are also meritless. First, the Fraud Reduction Claims do not limit capturing and analyzing information to a specific technological environment; the claims exist to address a problem *created by* the technological environment (an electronic payment network). And despite Apple's assertions to the contrary, the Fraud Reduction Claims do not merely recite using biometric information to make a determination, they claim a *new technique*—the "aliveness" determination—for performing biometric analysis to authenticate an electronic transaction.

It is also telling that Apple does not dispute that determining "aliveness" is an improvement over then-existing biometric authentication techniques. *See* Mot. 8-9. Rather, Apple attacks the "aliveness" determination by arguing that the claims do not show *how* aliveness is determined, meaning this new feature amounts to a functional abstraction or a "black box." *Id.* But the claims and specification *do* mention *how* to determine whether a user is

"alive"—*e.g.*, taking photos of the user in rapid succession to look for minor variations among the various captured images. *See* '010 Patent at cl. 21 and 8:58-8:60; '886 Patent at cls. 1, 6, 11, 14, and 20; *see TecSec*, 978 F.3d at 1292 (explaining courts ask "what the patent asserts to be the focus of the claimed advance over the prior art" considering the asserted claims "in light of the specification"). That said, ***how*** a person skilled in the art would implement a claimed invention is a § 112 enablement issue, not § 101 eligibility issue to be taken up on a motion to dismiss. *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1261 (Fed. Cir. 2017) ("[W]hether a patent specification teaches an ordinarily skilled artisan how to implement the claimed invention presents an enablement issue under 35 U.S.C. § 112, not an eligibility issue under § 101.").

**b) *Alice* Step Two: As alleged in the Complaint, the Fraud Reduction Claims recite inventive concepts.**

Because, as explained above, the Fraud Reduction Claims are not abstract, the Court need not go beyond step one. But even if it does, the claims are directed to an inventive concept and are therefore patent eligible under *Alice* step two. Patent claims recite an "inventive concept" if they reflect "something more than well-understood, routine, conventional activities previously known to the industry." *Cellspin Soft, Inc.*, 927 F.3d at 1315. The Fraud Reduction Claims do just that. By incorporating the "aliveness" determination into the biometric analysis, the claims go beyond what was known to the cybersecurity industry at the time, *e.g.*, basic photo-verification technology. *See* '010 Patent at 8:58-8:60. The Federal Circuit has held claims that provide similar advances over the prior art recite an inventive concept and are patent eligible. *CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091, 1099 (Fed. Cir. 2021) (finding claims reciting "improved method for overcoming hacking" were eligible at step two).

Apple argues that the claims do not support an inventive concept because they include conventional components or components recited in functional terms performing their

conventional functions in conventional methods. Mot. at 10-11. This is pure attorney argument. Apple has pointed to no evidence that authenticating an electronic transaction based on an analysis of a user's biometric information to determine the user is alive was well understood, routine, or previously known in the industry. Apple has certainly not provided clear and convincing evidence that this was the case. This failure of proof is reason enough to deny Apple's Motion. *Mytee Prod., Inc. v. Harris Rsch., Inc.*, 439 F. App'x 882, 884 (Fed. Cir. 2011) (rejecting invalidity arguments that are "little more than conclusory assertions, gross generalities, and unsupported assumptions made by counsel").[2]

But beyond Apple's failure of proof, the claims recite an inventive concept, for example, by incorporating the "aliveness" determination as part of the claimed biometric authentication process. *See* '010, '656, and '886 Patents at cl. 1. This was not a conventional feature in electronic payment authentication at the time of the invention (and Apple has not shown that it was), and it provided a discrete improvement over then-existing verification techniques that were known in the art—the hallmark of an inventive concept. At a minimum, the Complaint raises issues of fact over whether the Fraud Reduction Patents possess an inventive concept, *see* Compl. ¶¶ 57-61, meaning Apple's arguments should not be resolved at this early stage, and its Motion should be denied. *Aatrix Software*, 882 F.3d at 1128 (Whether claim elements "are well-understood, routine, conventional is a question of fact" that "cannot be answered adversely to the patentee based on the sources properly considered on a motion to dismiss.").

## IV. CONCLUSION

For the reasons set forth above, Apple's premature Motion should be denied.

---

[2] The Federal Circuit has also held that conventional computer components can recite an inventive concept. *BASCOM*, 827 F.3d at 1349-50.

Dated: June 14, 2023.

MCKOOL SMITH, P.C.

*/s/ Joshua W. Budwin*
Joshua W. Budwin
Lead Attorney
Texas State Bar No. 24050347
jbudwin@mckoolsmith.com
George T. Fishback, Jr.
Texas State Bar No. 24120823
gfishback@McKoolSmith.com
Caroline Burks
Texas State Bar No. 24126000
cburks@McKoolSmith.com
**MCKOOL SMITH, P.C.**
303 Colorado Street Suite 2100
Austin, TX 78701
Telephone: (512) 692-8700
Telecopier: (512) 692-8744

Richard A. Kamprath
Texas State Bar No. 24078767
rkamprath@McKoolSmith.com
Bradley Jarrett
Texas State Bar No. 24128518
bjarrett@mckoolsmith.com
**MCKOOL SMITH, P.C.**
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: (214) 978-4210

**ATTORNEYS FOR PLAINTIFF CARBYNE BIOMETRICS, LLC**

**CERTIFICATE OF SERVICE**

I hereby certify that a true and correct copy of the above and foregoing document has been served on all counsel of record via the Court's ECF system on June 14, 2023.

*/s/ Joshua W. Budwin*
Joshua W. Budwin