

Stephen Q. Wood (Utah Bar No. 12403)
stephenwood@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
2755 East Cottonwood Parkway, Suite 520
Salt Lake City, Utah 84121
Tel: (801) 515-7300
Fax: (801) 515-7400

Jonathan E. Pickhardt (*pro hac vice*)
jonpickhardt@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
295 5th Avenue, 9th Floor
New York, New York 10016
Tel: (212) 849-7000
Fax: (212) 849-7100

Todd M. Briggs (*pro hac vice*)
toddbriggs@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, California 94065
Tel: (650) 801-5000
Fax: (650) 801-5100

Christopher R. Sabbagh (*pro hac vice*)
chrissabbagh@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
700 Louisiana Street, Suite 3900
Houston, Texas 77002
Tel: (713) 221-7000
Fax: (713) 221-7200

Attorneys for Plaintiff
Secure Authentication Technologies LLC

**UNITED STATES DISTRICT COURT
DISTRICT OF UTAH**

SECURE AUTHENTICATION
TECHNOLOGIES LLC,

Plaintiff,

v.

PLAID INC.,

Defendant.

**OPPOSITION TO DEFENDANT PLAID
INC.'S MOTION TO DISMISS UNDER
FEDERAL RULE OF CIVIL
PROCEDURE 12(b)(6)**

Case No. 2:25-cv-00514-DAK-JCB

District Judge: Hon. Dale A. Kimball

Magistrate Judge: Hon. Jared C. Bennett

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. FACT BACKGROUND	3
A. U.S. Patent No. 11,315,090.....	3
B. Prosecution History.....	5
III. LEGAL STANDARDS	6
A. Motions to Dismiss Under Federal Rule of Civil Procedure 12(b)(6).....	6
B. Patent Eligibility Under 35 U.S.C. § 101.....	7
IV. ARGUMENT	8
A. <i>Alice</i> Step One.....	8
1. The Claims Recite a Technological Solution to a Technological Problem	8
2. Defendant Cannot Rebut SAT’s Allegations That Show the Claims Are Directed to a Technological Solution	11
3. Defendant Improperly Generalizes the Claims to Make Its Argument	13
4. Defendant’s Allegations That the Claims Use Only Generic Technology Contradict Fact and Law	14
B. <i>Alice</i> Step Two.....	16
1. The Claims Recite a Specific Improvement to Authentication	16
2. Defendant Cannot Rebut SAT’s Allegations That Show the Claims Require Significantly More than the Alleged Abstract Idea.....	17
3. Defendant Improperly Generalizes the Claims to Argue They Do Not Improve Authentication	18
4. Defendant’s Allegations That the Claims Use Only Generic Technology and Processes Contradict Fact and Law	20
C. Defendant’s Cases Are Procedurally and Substantively Distinguishable.....	21
D. If the Court Grants Defendant’s Motion, Dismissal Should Be Without Prejudice	25
V. CONCLUSION.....	25

TABLE OF AUTHORITIES

Cases

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018).....	8, 12, 15, 25
<i>AlexSam, Inc. v. HealthEquity, Inc.</i> , 477 F. Supp. 3d 1227 (D. Utah 2020).....	6, 7, 8, 11
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	7
<i>Ashgari-Kamrani v. U.S. Servs. Auto. Ass’n</i> , No. 2:15-cv-00478, 2016 WL 3670804 (E.D. Va. July 5, 2016).....	23
<i>Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016).....	21
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	6
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018).....	2, 7, 16, 17
<i>Blix Inc. v. Apple, Inc.</i> , No. 1:19-cv-01869-LPS, 2020 WL 7027494 (D. Del. Nov. 30, 2020)	23
<i>Boom! Payments, Inc. v. Stripe, Inc.</i> , 839 F. App’x 528 (Fed. Cir. 2021)	23
<i>Contour IP Holding LLC v. GoPro, Inc.</i> , 113 F.4th 1373 (Fed. Cir. 2024)	8, 9, 13, 15, 23
<i>Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.</i> , 880 F.3d 1356 (Fed. Cir. 2018).....	15, 16
<i>CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC</i> , 15 F.4th 1091 (Fed. Cir. 2021)	5, 24, 25
<i>cxLoyalty, Inc. v. Maritz Holdings Inc.</i> , 986 F.3d 1367 (Fed. Cir. 2021).....	21, 23
<i>DDR Holdings, LLC v. Hotels.com, LP</i> , 773 F.3d 1245 (Fed. Cir. 2014).....	9
<i>Diamond v. Chakrabarty</i> , 447 U.S. 303 (1980).....	7

<i>Fraud Free Transactions LLC v. Ping Identity Corp.</i> , 70 F. Supp. 3d 460 (D. Del. 2025).....	23
<i>InsideSales.com, Inc. v. SalesLoft, Inc.</i> , No. 2:16-cv-859-DAK, 2017 WL 2559932 (D. Utah June 13, 2017)	1, 7, 9, 10, 13, 16, 24
<i>Intellectual Ventures I LLC v. Capital One Bank (USA)</i> , 792 F.3d 1363 (Fed. Cir. 2015).....	9
<i>Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.</i> , 566 U.S. 66 (2012).....	7
<i>Playtex Prods., Inc. v. Procter & Gamble Co.</i> , 400 F.3d 901 (Fed. Cir. 2005).....	11
<i>PowerBlock Holdings, Inc. v. iFit, Inc.</i> , 146 F.4th 1366 (Fed. Cir. 2025)	9
<i>Prism Techs. LLC v. T-Mobile USA, Inc.</i> , 696 F. App’x 1014 (Fed. Cir. 2017)	23
<i>Samsung Elecs. Co. v. Blaze Mobile, Inc.</i> , 673 F. Supp. 3d 1066 (N.D. Cal. 2023)	23
<i>SAP America, Inc. v. InvestPic, LLC</i> , 898 F.3d 1161 (Fed. Cir. 2017).....	20
<i>Smart Authentication IP, LLC v. Elec. Arts Inc.</i> , 402 F. Supp. 3d 842 (N.D. Cal. 2019)	23
<i>Sylvia v. Wisler</i> , 875 F.3d 1307 (10th Cir. 2017)	7
<i>Torus Ventures LLC v. Cawley Partners, LLC</i> , No. 2:24-cv-00552-JRG, 2025 WL 1799327 (E.D. Tex. June 30, 2025).....	20
<i>Univ. of Fla. Res. Found., Inc. v. Gen. Elec. Co.</i> , 916 F.3d 1363 (Fed. Cir. 2019).....	9
<i>World Class Tech. Corp. v. Ormo Corp.</i> , 769 F.3d 1120 (Fed. Cir. 2014).....	11

Other Authorities

37 C.F.R. § 1.104	5
37 C.F.R. § 1.111	5
Federal Rule of Civil Procedure 12(b)(6)	6, 7, 8

I. INTRODUCTION

Defendant Plaid Inc.’s motion not only requires the Court to improperly reject Plaintiff Secure Authentication Technologies LLC’s well-pleaded fact allegations, it also asks the Court to decide highly technical fact issues—that should go to a jury in the normal course of litigation—without the benefit of expert testimony. Defendant tries to avoid the consequences of infringing SAT’s patent, but its attempt is premature and contravenes the applicable legal standards at this early stage of litigation, which require the Court to accept SAT’s allegations as true.

The Court has encountered this situation before. The defendant in *InsideSales.com, Inc. v. SalesLoft, Inc.*, No. 2:16-cv-859-DAK, 2017 WL 2559932 (D. Utah June 13, 2017) similarly asked this Court to invalidate a patent under 35 U.S.C. § 101 at the motion-to-dismiss stage. The Court refused the defendant’s request, explaining that “Section 101 has an expansive definition of patentability and Congress intended patent laws to ‘be given wide scope’” and that “[t]he exclusion for abstract ideas is applied narrowly.” *Id.* at *2 (citations omitted). “Because the court [had to] accept the well-pleaded factual allegations of the Complaint as true and construe them in the light most favorable to [the plaintiff], the court conclude[d] that [the defendant] ha[d] not proven the patents-in-suit to be patent ineligible under § 101” and denied the defendant’s motion. *Id.* at *4. The Court should do the same here because Defendant’s motion is both incorrect and inappropriate, especially in view of the allegations in SAT’s complaint. The claims of U.S. Patent No. 11,315,090 (“the ’090 patent”) are patent eligible.

This is not the classic case under *Alice* where a patent takes a long-standing process that humans performed without the use of computers, and then merely implements that process on a computer. Indeed, Defendant *never alleges* that the process described in the claims—collecting and encrypting credentials and using them to satisfy a multi-factor authentication request without user intervention—is a known practice that humans performed well before computers were

invented. Nor can it, as the problem and solution described in the '090 patent did not exist *before* computers, but rather arose *because of* computers: Multi-factor authentication exists only because it is difficult to authenticate a person over the Internet, where typical in-person authentication techniques—like verifying a person’s identity by looking at their driver’s license—are not viable. Accordingly, the patent claims here belong to a different class of claims that the Federal Circuit routinely finds eligible under § 101; claims that take a problem created by computers and solve the problem via a technical process that did not exist pre-computers. Thus, at *Alice* step one, the claims are not directed to an abstract idea because they provide a technological solution to a technological problem.

The Court need not reach *Alice* step two since the claims are not directed to an abstract idea. But should the Court analyze this step, the claims still survive *Alice* because they recite a specific improvement to the authentication process that goes beyond the alleged abstract idea. This step involves a “question of fact” that asks whether the claims were well-understood, routine, or conventional. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). So SAT’s well-pleaded allegations defeat Defendant’s motion because they confirm the patent describes a “unique and inventive” solution. Complaint ¶ 13. Not surprisingly, Defendant never addresses these allegations head on. Instead, Defendant resorts to baseless accusations, alleging that SAT’s complaint is “conclusory” and “divorced from the claims.” Dkt. 29 (“Mot.”), at 24. SAT’s allegations are not conclusory and find support in both the patent’s claims and specification, which require hardware capable of securely encrypting and sending sensitive data in an inventive manner.

Defendant provides no compelling reason to disregard SAT’s fact allegations. Instead, Defendant misrepresents the patent and the law so it can continue to infringe SAT’s patent. The

Court should deny Defendant’s motion, as it did in *InsideSales.com*, and allow the parties to develop their arguments through discovery and claim construction, and present them to a jury.

II. FACT BACKGROUND

A. U.S. Patent No. 11,315,090

The ’090 patent claims a foundational innovation in financial technology. At the time of the invention,¹ some financial institutions—and even more, now—required “multi-level or multi-factor authentication protocols” to access an account. ’090 patent at 17:64–18:6. For example, these financial institutions would prompt an individual to input an authentication code, which the institution had sent to the account holder via text message or e-mail, before allowing the individual to access the requested account. *Id.* at 18:7–23.

Although multi-factor authentication promoted account security, it also prevented financial management systems from freely accessing the individual’s accounts to retrieve and display current balance information. Complaint ¶ 12. In order for the system to work on an ongoing basis, the individual would need to provide an authentication code every time the financial management system accessed any of the individual’s accounts that were protected by such protocols. *Id.*

This problem prevented the development and operation of innovative financial management systems, which could not access an individual’s financial accounts without repeatedly prompting that person for authentication codes. *See* ’090 patent at 1:33–3:6. The patent therefore discloses that, “with respect to multi-factor authentication, the financial management network implements unique and inventive concepts that permit it to act as proxy for the user” and “respond to any multi-factor authentication that may be required for account access in a way that

¹ The ’090 patent claims priority to a provisional patent application filed on January 28, 2014. ’090 patent at 1:4–14.

does not require user intervention, while simultaneously maintaining rigid security measures to avoid unauthorized access to the user's accounts by other parties." *Id.* at 18:53–60.

Specifically, "[w]hen a user first links an account to the financial management network, the user supplies their username and password to the financial management network, and a process within the financial management network" attempts to log in to the user's account. *Id.* at 19:29–34. "If the bank responds to the log in attempt by issuing challenge questions or by requiring additional multi-factor authentication such as entry of a code sent to the user, then the financial management network will prompt the user for the additional information that the bank website has requested." *Id.* at 19:35–40. One embodiment of this technological solution is disclosed in claim 1 of the '090 patent:

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Id. at 30:61–31:18. Once the financial management network has access to the account, it can further "add[] to the user data stored by the site an additional multi-factor authentication endpoint, e.g., an additional phone number or email address" to facilitate any subsequent multi-factor

authentication requests. *Id.* at 19:60–67. One embodiment of this technological solution is disclosed in claim 2 of the ’090 patent:

2. The method of claim 1, further comprising the steps of:

storing one or more of the account holder’s endpoints for the online account in a data store associated with the online account; and

utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.

Id. at 31:19–27.

B. Prosecution History

Before it issued, the application resulting in the ’090 patent spent two years being examined by the United States Patent and Trademark Office in a process known as patent prosecution. *See generally* Dkt. 1-2 (prosecution history). Patent prosecution is a back-and-forth process in which an examiner, who is trained in the technical field of the invention, either accepts or rejects a patent application in view of potential eligibility issues. *See* 37 C.F.R. § 1.104. If rejected, the applicant has the opportunity to either directly refute the examiner’s rejection or amend the patent’s claims to sidestep the rejection. *See* 37 C.F.R. § 1.104(c); 37 C.F.R. § 1.111.

The patent examiner here raised and then rejected the very issue that Defendant asserts in its motion. On June 11, 2021, the examiner initially asserted that the ’090 patent’s claims were directed to ineligible subject matter under 35 U.S.C. § 101. Dkt. 1-2 at 97–106.

The applicant responded on January 30, 2022, explaining that the claims were eligible under § 101 in view of the Federal Circuit’s recent (at that time) decision in *CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC*, 15 F.4th 1091 (Fed. Cir. 2021). *Id.* at 29–33. The applicant explained that “[t]his solution, disclosed by Applicant’s claimed methods, can only be implemented using specialized computer hardware.” *Id.* at 29. For example, “specialized

computer systems are required to implement 256-bit bank-level encryption to protect these login credentials, which is the only known safe and trusted way to transmit and store such credentials” and “specialized computer hardware is necessary to power the headless browsers that are able to use logic to interpret bank websites and interact with their various messages, prompts, data input boxes, and action buttons.” *Id.* Further, “a human call center could not serve this function, for no savvy bank customer would ever provide their unencrypted username/password combination necessary to access their bank account to another untrusted human – in fact, doing so would violate the agreement that exists between a bank and its customers.” *Id.*

In short, the applicant explained that the claims disclose patentable subject matter because they “leverag[e] specialized computer hardware and software, computer logic, and encryption, to overcome a method of security that was intended to be impenetrable.” *Id.* at 30. The applicant further explained that—to the extent the examiner maintained that the claims are abstract—“the pending claims nonetheless are patent eligible as having significantly more than an abstract idea” by “recit[ing] the use of an encrypted process that helps individual investors manage, in a secure way, a multitude of bank accounts through a single interface.” *Id.* at 31–32.

Agreeing with the applicant, the examiner reversed his initial determination and concluded that the claims “qualify as patent eligible subject matter” on March 11, 2022. *Id.* at 9–10.

III. LEGAL STANDARDS

A. Motions to Dismiss Under Federal Rule of Civil Procedure 12(b)(6)

A defendant’s motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) fails if the plaintiff’s complaint contains “enough facts to state a claim to relief that is plausible on its face.” *AlexSam, Inc. v. HealthEquity, Inc.*, 477 F. Supp. 3d 1227, 1230 (D. Utah 2020) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is

liable for the misconduct alleged.” *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). When deciding a Rule 12(b)(6) motion, courts “must accept all the well-pleaded allegations of the complaint as true and must construe them in the light most favorable to the plaintiff.” *Id.* (cleaned up in original) (quoting *Sylvia v. Wisler*, 875 F.3d 1307, 1313 (10th Cir. 2017)).

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

Under 35 U.S.C. § 101, “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof” is eligible for patenting. “Section 101 has an expansive definition of patentability and Congress intended patent laws to ‘be given wide scope.’” *InsideSales.com*, 2017 WL 2559932, at *2 (quoting *Diamond v. Chakrabarty*, 447 U.S. 303, 308–09 (1980)). “However, there are exceptions to patentability,” including that “abstract ideas are not patentable.” *Id.*

“The exclusion for abstract ideas is applied narrowly.” *InsideSales.com*, 2017 WL 2559932, at *2 (citing *Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.*, 566 U.S. 66, 71 (2012)). “[T]oo broad an interpretation of this exclusionary principle would undermine patent law,’ because ‘all inventions at some level[embody,] use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.’” *Id.* (quoting *Mayo*, 566 U.S. at 71). “Courts, therefore, have been directed to ‘tread carefully in construing this exclusionary principle lest it swallow all of patent law.’” *Id.* (quoting *Alice*, 573 U.S. at 217).

Additionally, “[t]he patent eligibility inquiry may contain underlying issues of fact.” *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018). For example, “[t]he question of whether 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.” *Id.* at 1368. “‘At the Rule 12(b)(6) stage,’ the court can determine patent eligibility” under 35 U.S.C. § 101 “‘only when there are no factual allegations that prevent resolving the eligibility question as a matter of law.’” *AlexSam*,

477 F. Supp. 3d at 1230–31 (cleaned up in original) (quoting *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018)). “‘Plausible factual allegations’ may thus ‘preclude dismissing a case [for patent ineligibility] where nothing on the record refutes those allegations as a matter of law or justifies dismissal under Rule 12(b)(6).’” *Id.* at 1231 (alteration in original) (quoting *Aatrix*, 882 F.3d at 1125).

IV. ARGUMENT

Defendant’s motion to dismiss does not heed the Supreme Court’s directive to “tread carefully in construing” patent eligibility under § 101 “lest it swallow all of patent law.” *Alice*, 573 U.S. at 217. To the contrary, Defendant asks the Court to uproot deep-seated legal standards—by acting as fact finder and denying SAT’s fact allegations without the benefit of expert testimony or jury input. This is not a case in which the intrinsic record (like the patent and claims themselves) contradicts the plaintiff’s allegations and confirms that the claimed process has long been performed by humans. This case is on the other end of the spectrum. The ’090 patent explains that the claims are rooted in computer technology and novel, and the claimed process itself confirms that it has not long been performed by humans. The Court should deny Defendant’s motion.

A. *Alice* Step One

1. The Claims Recite a Technological Solution to a Technological Problem

Claims, like the claims here, that are “directed to a technological solution to a technological problem” “recite patent-eligible subject matter at *Alice* step one.” *Contour IP Holding LLC v. GoPro, Inc.*, 113 F.4th 1373, 1380–81 (Fed. Cir. 2024). The typical case under *Alice* involves a patent that takes a long-standing practice that humans have performed without the benefit of computers and then implements that practice on a computer. *See infra* § IV.C. This ***is not*** that case, as the problem and solution described in the ’090 patent did not exist before computers but

rather arose because of computers. This Court has previously explained that “Federal Circuit law is clear in rejecting § 101 challenges where a patent’s ‘claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.’” *InsideSales.com*, 2017 WL 2559932, at *3 (quoting *DDR Holdings, LLC v. Hotels.com, LP*, 773 F.3d 1245, 1247 (Fed. Cir. 2014)). “Inventions that ‘provide[] an Internet-based solution to solve a problem unique to the Internet’ are not unpatentable abstract ideas.” *Id.* (alteration in original) (quoting *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1371 (Fed. Cir. 2015)). Instead, they are a “technological solution to a technological problem” that are patent eligible under *Alice*. *Contour*, 113 F.4th at 1373.

The ’090 patent solves such a technological problem, necessarily placing it outside the universe of “abstract” solutions. The Federal Circuit has explained that a hallmark indicator of whether claims are directed to an abstract idea is if the claims merely automate a process that has been historically performed by humans in the real world. *PowerBlock Holdings, Inc. v. iFit, Inc.*, 146 F.4th 1366, 1372 (Fed. Cir. 2025). Defendant does not argue that the patent here is such “a quintessential ‘do it on a computer’ patent” or that the claimed solution existed before computers were invented. *Id.* (quoting *Univ. of Fla. Res. Found., Inc. v. Gen. Elec. Co.*, 916 F.3d 1363, 1366–67 (Fed. Cir. 2019)). For example, Defendant does not assert that humans—in brick-and-mortar stores before the advent of computers—used to perform the claimed processes to work around multi-factor authentication in a secure manner.²

² At best, Defendant suggests in footnote that the patent analogizes the claims to a “limited power of attorney.” Mot. 10 n.3. Defendant’s footnote misrepresents what the patent says. The patent merely notes that the system can optionally execute “a limited power of attorney” to establish legal authority to access the account, “to the extent necessary.” ’090 patent at 18:60–64. A limited power of attorney is not intended to address (nor does it solve) the technical problems created by multi-factor authentication and is thus not analogizable to the claims.

Nor can it. Computers and the Internet *created* the problems that the '090 patent solves. As the patent explains, “multi-factor authentication protocols may involve *a bank’s website* indicating that it will be transmitting a pre-determined or random authentication code,” which is often sent “*by email* to the user’s email address.” ’090 patent at 18:12–16 (emphasis added). This protocol is used to verify “login[s] from an unauthorized *client computer*.” *Id.* at 18:7–12 (emphasis added); *see also id.* at 19:21–20:14 (explaining how multi-factor authentication is used to enable access to online accounts). In other words, the claims here address the need to securely verify an individual’s identity online, where traditional in-person methods proved ineffective. Defendant therefore cannot claim that this is a “longstanding business practice” that the claims merely implement on a computer. *InsideSales.com*, 2017 WL 2559932, at *2. As SAT pleaded in its complaint, “a human call center” simply “could not serve this function, for no savvy bank customer would ever provide their unencrypted username/password combination necessary to access their bank account to another untrusted human – in fact, doing so would violate the agreement that exists between a bank and its customers.” Complaint ¶ 15; *see also* Dkt. 1-2, at 30.

Further, the solution disclosed in the '090 patent can only be implemented using specialized computer hardware. SAT explained in its complaint that ordinary computers cannot implement the claims because “specialized computer systems are required to implement 256-bit bank-level encryption to protect [a user’s] login credentials, which is the only known safe and trusted way to transmit and store such credentials.” Complaint ¶ 15; *see also* Dkt. 1-2, at 30. Additionally, “specialized computer hardware is necessary to power the headless browsers that are able to use logic to interpret bank websites and interact with their various messages, prompts, data input boxes, and action buttons.” Complaint ¶ 15; *see also* Dkt. 1-2, at 30. The claims “leverag[e] specialized computer hardware and software, computer logic, and encryption, to overcome a

method of security that was intended to be impenetrable.” Dkt. 1-2, at 30. The claims are therefore not abstract because they solve a technological problem in a technological manner.

2. Defendant Cannot Rebut SAT’s Allegations That Show the Claims Are Directed to a Technological Solution

SAT’s complaint pleads facts sufficient to show that the claims are directed to a technological solution, not an abstract idea. It is well-established that a court must accept a plaintiff’s well-pleaded allegations as true at this stage. *AlexSam*, 477 F. Supp. 3d at 1230. As discussed above, SAT’s complaint pleads that the claims are directed to a technological solution because they use specialized computer technology and cannot be implemented by humans. *See* Complaint ¶¶ 12–16.

Defendant’s argument that SAT does not show that the claims improve an “existing technological process” and “employ only generic technology” is simply wrong. Mot. 14–15. SAT explained that the claims improve the process of authenticating a user such that third parties can access accounts despite the presence of multi-factor authentication, Complaint ¶¶ 11–14, and SAT further explained that the claims require specialized computer components, *id.* ¶¶ 15–16. Defendant does not rebut these allegations.

Further, Defendant’s argument that the claims require only generic components also ignores that the meaning of a patent’s claims are informed by “the specification particularly, but also the prosecution history.” *World Class Tech. Corp. v. Ormo Corp.*, 769 F.3d 1120, 1123 (Fed. Cir. 2014). Courts derive this meaning during a process called claim construction, which often rests on expert testimony about how a skilled artisan would interpret claims when considering the specification, prosecution history, and general knowledge of the field. *See Playtex Prods., Inc. v. Procter & Gamble Co.*, 400 F.3d 901, 908 n.1 (Fed. Cir. 2005) (“It is appropriate for courts engaged in claim construction to consider expert testimony.”). Defendant tries to bypass claim

construction (1) by arguing that the claims require only generic computer components in contravention of the specification and prosecution history and (2) without giving the Court an opportunity to properly construe the claims and consider expert testimony that will, if needed, shed light on the claims' meaning. To the extent there is any dispute about what kind of "processors" the claims require or what the "encrypting" limitation entails, "the court must proceed by adopting the non-moving party's constructions"—here, that the "processors" are specialized processors that can implement the "encrypting" limitation, which requires 256-bit bank-level encryption and headless browsing—or by resolving claim construction first. *Aatrix*, 882 F.3d at 1125.

Defendant, acknowledging that it cannot rebut SAT's allegations, characterizes them as "conclusory." Mot. 4–5, 20–21. These are not conclusory allegations nor are they "unsupported by specific factual allegations." *Id.* at 21. They do not "simply parrot[] the claim language and label[] routing computer functions . . . as a 'technological solution.'" *Id.* To the contrary, these allegations specifically plead that ordinary computers cannot "implement 256-bit bank-level encryption to protect [a user's] login credentials, which is the only known safe and trusted way to transmit and store such credentials"; that "specialized computer hardware is necessary to power the headless browsers that are able to use logic to interpret bank websites and interact with their various messages, prompts, data input boxes, and action buttons"; and that "a human call center could not serve this function, for no savvy bank customer would ever provide their unencrypted username/password combination necessary to access their bank account to another untrusted human – in fact, doing so would violate the agreement that exists between a bank and its customers." Complaint ¶ 15.

Should Defendant wish to rebut these allegations, that is the purpose of discovery and trial, not a motion to dismiss. The Court arrived at this conclusion in *InsideSales.com*: "Because the

court must accept the well-pleaded factual allegations of the Complaint as true and construe them in the light most favorable to InsideSales, the court concludes that SalesLoft has not proven the patents-in-suit to be patent ineligible under § 101.” *InsideSales.com*, 2017 WL 2559932, at *4. Similarly here, the Court should deny Defendant’s motion for this reason alone and allow the parties to further develop the record on this issue in the ordinary course of litigation.

3. Defendant Improperly Generalizes the Claims to Make Its Argument

Defendant also ignores the details of the claims to argue that they are abstract. Describing the claims as merely “using a third-party intermediary to facilitate a transaction,” Mot. 9, “characterizes the claims at an impermissibly high level of generality,” *Contour*, 113 F.4th at 1379–80. By Defendant’s design, this broad characterization ignores the technical details that make the claims non-abstract. For example, it ignores the requirements of “encrypting the account holder’s credentials using one or more processors” and “storing one or more of the account holder’s endpoints for the online account in a data store associated with the online account,” which as a result “disregards the disclosed technological means for obtaining a technological result.” *Id.* Such a “generalized articulation of the claimed advance of the claims” should be rejected because it “all but ensure[s] the incorrect conclusion that the claims were drawn to an abstract idea.” *Id.* More accurately, the claims are directed to the technological solutions of enabling a third-party to gain secure access to online accounts that are otherwise protected by a multi-factor authentication protocol (Claim 1), and enabling future access without requiring the account holder to be present (Claim 2), as SAT pleaded in its complaint. Complaint ¶ 11.

Defendant continues to impermissibly generalize the claims when it argues the claims “employ purely functional language.” Mot. 15–16. Defendant relies on sleight of hand to make this argument. Defendant lists out terms that it says are “purely functional,” including the term “encrypting.” Mot. 15. But then Defendant omits “encrypting,” in the very next sentence, from a

second list of terms that can be purportedly carried about by “a human . . . in their mind or with a pen and paper.” *Id.* at 15–16. By omitting “encrypting” from this second list, Defendant appears to admit that the claims *do* recite particular requirements for encrypting that *cannot* be performed by a human with a pen and paper. In fact, that is the very point SAT made through factual allegations in its complaint. The claims use specialized computer technology to perform this encryption that cannot be performed by a human. Complaint ¶¶ 12–16. Defendant’s motion therefore fails to address the key point at issue and should be denied.

Finally, this argument tries to bypass important stages of patent litigation, arguing about what the claims require before the parties have briefed claim construction. *See supra* § IV.A.2. Defendant’s arguments are therefore unpersuasive because they strategically ignore the substance of the ’090 patent and ask the Court to construe claims without the benefit of a full record.

4. Defendant’s Allegations That the Claims Use Only Generic Technology Contradict Fact and Law

Finally, Defendant’s argument that the hardware required by the claims are “generic components” or “generic technology” not only impermissibly contradicts SAT’s fact allegations but also misunderstands the § 101 inquiry. SAT explained in its complaint that the claims “can only be implemented using specialized computer hardware” that can “implement 256-bit bank-level encryption to protect these login credentials, which is the only known safe and trusted way to transmit and store such credentials,” and that can “power the headless browsers that are able to use logic to interpret bank websites and interact with their various messages, prompts, data input boxes, and action buttons.” Complaint ¶ 15 (quoting Dkt. 1-2, at 29–30). Defendant’s argument that the processor in the claims can be “generic” therefore contradicts SAT’s well-pleaded facts, which the Court must accept as true.

The patent specification supports SAT’s fact allegations. The claims themselves require the processor to securely encrypt the account holder’s credentials. *See* ’090 patent at 31:1–2. The specification supports this requirement, explaining the invention must be implemented on a “financial management system” that must include “a processor” that is able to “implement[] the desired transactions.” *Id.* at 3:64–4:3. These transactions include “multiple processes that permit an account holder to access account information across his various accounts and that permit the financial management network to interface with banks holding the one or more user accounts, and in particular to permit the financial management network to login as the user by using the user’s credentials stored in credential data store.” *Id.* at 18:65–19:6. SAT’s complaint pleads that generic processors cannot carry out these functions securely. Complaint ¶ 15. As explained above, a patent’s claims are interpreted in view of both the specification and a skilled artisan’s general knowledge, *see supra* § IV.A.2, and this information will be reflected in the record via forthcoming claim construction and expert reports. At this point in litigation, the Court “must proceed by adopting [SAT’s] constructions” that require non-generic processors and a particular form of encryption. *Aatrix*, 882 F.3d at 1125.

Further, even if the claims could be performed by generic components, that still would not mean the claims are directed to an abstract idea. The Federal Circuit recently rejected a similar argument “contend[ing] that the claims simply employ known or conventional components” and are therefore directed to an abstract idea. *Contour*, 113 F.4th at 1380. “Even so,” the Federal Circuit said, “that *alone* does not necessarily mean that the claim is *directed to* an abstract idea at step one.” *Id.* (emphases in original) (citing *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1362 (Fed. Cir. 2018)). Even a system that “use[s] conventional” components is

eligible when it specifies “a particular method” that “eliminate[s] many of the complications inherent in conventional methods,” as here. *Core Wireless*, 880 F.3d at 1362.

B. *Alice* Step Two

1. The Claims Recite a Specific Improvement to Authentication

The Court need not analyze *Alice* step two because, as shown above, the claims are not directed to an abstract idea under *Alice* step one. *InsideSales.com*, 2017 WL 2559932, at *3. Should the Court decide that the claims are merely directed to using a third-party intermediary to facilitate a transaction, then the claims are nevertheless eligible under *Alice* step two because they recite a particular improvement to authentication that is “significantly more” than the alleged abstract idea itself. *Alice*, 573 U.S. at 217–18. Specifically, the authentication process described in the claims was not “well-understood, routine, and conventional to a skilled artisan in the relevant field,” and it leverages specialized computer components to perform that process. *Berkheimer*, 881 F.3d at 1368. “Whether something is well-understood, routine, and conventional to a skilled artisan at the time of the patent is a factual determination.” *Id.* at 1369.

Like the patent in *Berkheimer*, which “describe[d] an inventive feature” performed “in a purportedly unconventional manner,” *id.*, the patent here explains that the “network implements unique and inventive concepts that permit it to act as proxy for the user and respond to any multi-factor authentication . . . in a way that does not require user intervention, while simultaneously maintaining rigid security measures to avoid unauthorized access to the user’s accounts by other parties,” ’090 patent at 18:53–60 (citation omitted). To do this, the claims “leverag[e] specialized computer hardware and software, computer logic, and encryption, to overcome a method of security that was intended to be impenetrable.” Dkt. 1-2, at 30. Indeed, the United States Patent and Trademark Office (“USPTO”) would not have issued the ’090 patent if the patent did not disclose a “new and useful process.” 35 U.S.C. § 101. These improvements “create a factual

dispute regarding whether the invention describes well-understood, routine, and conventional activities.” *Berkheimer*, 881 F.3d at 1369. Although Defendant states in conclusory fashion that the claim elements “considered individually or in combination . . . are basic functions,” Defendant provides no support for this statement, which is just attorney argument. Mot. 20.

2. Defendant Cannot Rebut SAT’s Allegations That Show the Claims Require Significantly More than the Alleged Abstract Idea

SAT’s complaint pleads facts—which this Court must accept as true at this stage—that show the claims require significantly more than the alleged abstract idea because they were not well-understood, routine, or conventional. The Federal Circuit has explained that “whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field” under *Alice* step two is a “question of fact.” *Berkheimer*, 881 F.3d at 1368 (Fed. Cir. 2018)). Both the prosecution history, the patent itself, and SAT’s complaint explain how the claimed steps are inventive. Complaint ¶¶ 12–16; *see generally* Dkt. 1-2.

For example, SAT alleged that multi-factor authentication, at that time, prevented “financial management system[s] from freely accessing [] users’ accounts to retrieve and display current balance information which was necessary to re-distribute and optimize the users’ financial assets.” Dkt. ¶ 12. SAT further explained—quoting the patent itself—that the patent discloses a “financial management network” that “‘implements unique and inventive concepts that permit it to act as a proxy for the user’ and optionally ‘respond to any multi-factor authentication that may be required for account access in a way that does not require user intervention, while simultaneously maintaining rigid security measures to avoid unauthorized access to the user’s accounts by other parties.’” *Id.* ¶ 13 (quoting ’090 patent at 18:53–60 (citation omitted)). Finally, the examiner analyzed several prior-art references during prosecution and found that they “do[] not teach” various aspects of the ’090 patent’s claims. *See* Dkt. 1-2, at 11–12.

Defendant appears to recognize that it cannot rebut these allegations at this stage, so it does not even try. These well-pleaded allegations of “unique and inventive concepts” that can “respond to any multi-factor authentication . . . while simultaneously maintaining rigid security measures to avoid unauthorized access to the user’s accounts by other parties” in order to “overcome a method of security that was intended to be impenetrable” therefore defeat Defendant’s motion alone. Complaint ¶ 13 (quoting ’090 patent at 18:53–60 (citation omitted)); Dkt. 1-2, at 30.

3. Defendant Improperly Generalizes the Claims to Argue They Do Not Improve Authentication

The only way Defendant is able to argue that the claims do not improve authentication is to generalize the claims by arguing that they merely describe acting as a proxy for a user. Mot. 20–21. Again, this generalization erases significant and inventive technical detail from the claims; indeed, it erases the entire point of the claims, which is to improve the multi-factor authentication process in a manner that prevents unauthorized access by other third parties. *See supra* § IV.A.3. SAT made several factual allegations in the complaint supporting this point, which Defendant ignores. *Id.*

Defendant repeatedly states that SAT’s allegations are “conclusory” when they are not. The complaint explains in detail why the claims improve the conventional authentication process and why the claims are technical in nature, including by identifying the specific procedures that require specialized computer components—*i.e.*, encrypting login credentials and powering headless browsers. *See* Complaint ¶¶ 12–16. It is **Defendant’s** arguments that are conclusory.³ Defendant baselessly states that SAT’s allegations “‘cannot defeat a motion to dismiss’ because

³ It is difficult to discern what Defendant is referring to when it says “Plaintiff’s cited disclosures are the same as those discussed above with respect to Step One.” Mot. 21. SAT’s complaint does not include a step-by-step *Alice* analysis (which is not required by law or statute), so it is unclear what Defendant is referring to when it says SAT’s allegations for step two mirror its allegations for step one.

they are conclusory or ‘wholly divorced from the claims [and] the specification.’” Mot. 24 (alteration in original). Defendant does not even try to explain how the above factual allegations are “conclusory” when they are explained in more-than-sufficient detail, nor does Defendant explain how these allegations are “wholly divorced from the claims and the specification” when they are in fact supported by both. *See supra* § IV.A.4 (explaining that both the claims and specification require processors to securely manage a user’s login credentials). Similarly, Defendant makes other conclusory statements to make its case, like stating that “all the ’090 patent claims are basic functions” when considered “in combination” despite never analyzing the claims in combination nor providing factual support that each step in isolation is conventional. Mot. 20.

Considering SAT’s allegations fully and fairly—rather than perfunctorily discarding them as “conclusory,” as Defendant asks—it is evident the claims improve authentication in a technological manner. That is exactly what the examiner concluded after considering this very argument during prosecution: The claims “apply or use the judicial exception in some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment.” Complaint ¶ 16 (quoting Dkt. 1-2, at 9–10). Although not necessary to support this point, it is pertinent that the examiner—a technically trained individual who routinely reviews patent applications for this very issue—agreed with SAT. Complaint ¶¶ 15–16.

Defendant is correct that prosecution history is not binding on this Court, Mot. 21–22,⁴ but that history is still persuasive. Indeed, the applicant explained these very points to the examiner,

⁴ However, it is incorrect and an exaggeration for Defendant to argue that “the mere withdrawal of a Section 101 rejection during prosecution of a patent application does not require a holding of patent eligibility in the courts” because “[i]f that were true, all of the Federal Circuit and trial court decisions holding claims of issued patents patent ineligible would be wrong.” Mot. 21. Defendant has not shown that “all of the Federal Circuit and trial court decisions” on this issue involve an initial § 101 rejection that was later overturned, as here.

who withdrew his initial rejection under § 101 in view of this explanation. Complaint ¶¶ 15–16. Defendant cannot waive away the persuasive fact that an examiner, trained in this field of technology and familiar with § 101 rejections, allowed the claims in view of this explanation.

4. Defendant’s Allegations That the Claims Use Only Generic Technology and Processes Contradict Fact and Law

The claims here do not use generic technology or recite a generic procedure. Mot. 17–18, 23. Regarding technology, SAT’s allegations show that generic processors cannot implement the claims. *See supra* § IV.A.4.

Regarding procedure, Defendant does not show that the steps in the claims are “basic functions,” which lacks any fact support and is therefore conclusory. Mot. 17. The claims here are not merely analyzing data and displaying the results of an analysis, as in *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1167 (Fed. Cir. 2017). Mot. 17–18. There, the claims recited “nothing but a series of mathematical calculations.” *SAP*, 898 F.3d at 1163. Defendant does not allege that the claims here simply calculate numbers. Far from it. The claims here establish a secure way to access a user’s account that is protected by multi-factor authentication. And even if Defendant could reduce the claims to mere encryption, its argument that encrypting data “has been done for hundreds of years” comes from a non-precedential district court case in the Eastern District of Texas that cites to attorney argument made during a hearing. *See Torus Ventures LLC v. Cawley Partners, LLC*, No. 2:24-cv-00552-JRG, 2025 WL 1799327, at *6 (E.D. Tex. June 30, 2025) (citing Hearing Transcript, *Torus Ventures*, No. 2:24-cv-00552-JRG, Dkt. 73, at 9:1–2 (May 31, 2025)).

Even if Defendant could show that the claimed steps were well-known in isolation, Defendant has failed to show that they are well-known in combination. The Federal Circuit has made clear that the relevant inquiry at *Alice* step two is whether the steps are inventive “both

individually *and ‘as an ordered combination.’*” *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1347–48 (Fed. Cir. 2016) (emphasis added) (quoting *Alice*, 573 U.S. at 217). In *Bascom*, for example, the Federal Circuit reversed a district court’s decision to invalidate a patent under § 101 precisely because “[t]he district court looked at each limitation individually” without considering them “as an ordered combination.” *Id.* at 1349. Here, Defendant never mentions the limitations as an ordered combination other than to state in conclusory fashion that the limitations “considered individually or in combination . . . are basic functions.” Mot. 20. This lone conclusory sentence is not enough to defeat SAT’s allegations that the claims teach an inventive technological solution.

C. Defendant’s Cases Are Procedurally and Substantively Distinguishable

The opinions Defendant primarily relies on (*Alice*, *Universal Secure Registry*, and *cxLoyalty*) are procedurally distinguishable because many of them do not address motions to dismiss, and they are substantively distinguishable because they do not involve the technology at issue in this case.

Regarding procedure, two of the three cases that Defendant primarily relies on do not address a motion to dismiss and therefore did not need to grapple with the legal requirements that the Court must consider in resolving this motion, including the requirement to construe well-pleaded factual allegations in SAT’s favor and presume they are true. The district court in *Alice* resolved the issue following “cross-motions for summary judgment.” *Alice*, 573 U.S. at 214. Meaning, the district court decided this issue after claim construction, discovery, and expert reports that all informed whether the claims were eligible. The decision in *cxLoyalty* was issued through a now-defunct process called “covered business method review,” in which a panel of administrative judges—who have significant technical and patent experience—would review the eligibility of patents that the USPTO had previously issued. *cxLoyalty, Inc. v. Maritz Holdings*

Inc., 986 F.3d 1367, 1370 (Fed. Cir. 2021). This process also involved expert testimony, which the panel relied on in making its decision. *Id.* at 1375–76. These decisions are therefore categorically inapplicable because the Court does not have the benefit of a similarly complete record. Instead, Defendant asks the Court to hastily invalidate a patent contrary to SAT’s factual allegations and absent expert testimony.

The only case with a similar posture, then, is *Universal Secure Registry*, which is distinguishable on its facts. The patent there⁵ disclosed entering a “secret code” to purchase goods rather than presenting a credit card, which could risk “revealing personal financial information to a merchant,” *id.* at 1348, similar to how an elementary-school student might enter an assigned code when purchasing school lunch instead of carrying his parent’s credit card to school with him. Unsurprisingly, the Federal Circuit found, and “the patent itself acknowledge[d],” that this process of generating “codes for authentication of a user is conventional and long-standing,” and the patentee merely implemented it on a computer. *Id.* at 1350. In stark contrast, the claimed process here is not conventional or longstanding; the problem and solution did not exist *before* computers, but rather arose *because of* computers. *See* Complaint ¶¶ 12–14 (describing the circumstances in which multi-factor authentication is used and how the solution is implemented).

Defendant is only able to argue that the claims are longstanding by generalizing the invention to ignore technical aspects of the claims. *See supra* § IV.A.3. But the claims do not merely facilitate a transaction in a way that was known before computers existed. *Id.* Instead, they enable secure access to online accounts—a technological solution—protected by multi-factor

⁵ *Universal Secure Registry* involved “four asserted patents.” 10 F.4th at 1345. Defendant appears to rely only on the Federal Circuit’s analysis of the first patent. *See* Mot. 11 (citing only pages 1349 and 1350 of the decision).

authentication—an obstacle created by technology. *Id.* Such a “technological solution to a technological problem” is patent eligible. *Contour*, 113 F.4th at 1380–81.

In fact, all cases cited in Defendant’s motion are distinguishable on the merits for this reason—the problems and solutions in those patents existed long before computers, so there was no plausible dispute that the claims were directed to conventional and well-understood solutions that were not rooted in technology. *See Alice*, 573 U.S. at 219 (“Like the risk hedging in *Bilski*, the concept of intermediated settlement **is a fundamental economic practice long prevalent** in our system of commerce.” (emphasis added) (internal quotations omitted)); *cxLoyalty*, 986 F.3d at 1377 (“Humans have **long intermediated these very transactions** by collecting and relaying the very same information.” (emphasis added)); *Boom! Payments, Inc. v. Stripe, Inc.*, 839 F. App’x 528, 532 (Fed. Cir. 2021) (“We agree with Stripe that the claims are directed to the abstract idea of payment escrow” that existed pre-computers.); *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App’x 1014, 1017 (Fed. Cir. 2017) (finding persuasive “various **pre-computer-age corollaries** for which humans similarly restrict and provide access to resources” (emphasis added)); *Fraud Free Transactions LLC v. Ping Identity Corp.*, 70 F. Supp. 3d 460, 472 (D. Del. 2025) (“This claim merely invokes generic processes and machinery to attempt to monopolize a **longstanding method of organizing human activity**” of “identity verification from multiple sources to prevent fraud.” (emphasis added)); *Blix Inc. v. Apple, Inc.*, No. 1:19-cv-01869-LPS, 2020 WL 7027494, at *4 (D. Del. Nov. 30, 2020) (“As Apple demonstrates, every step recited in claim 17 **can be performed**, for example, **by a lawyer** representing a client who wishes to sell goods anonymously.”).⁶

⁶ *See also, e.g., Samsung Elecs. Co. v. Blaze Mobile, Inc.*, 673 F. Supp. 3d 1066, 1076 (N.D. Cal. 2023) (determining the claims were directed to “a fundamental economic practice”); *Smart Authentication IP, LLC v. Elec. Arts Inc.*, 402 F. Supp. 3d 842, 850 (N.D. Cal. 2019) (“Fundamental economic and conventional business practices are often found to be abstract ideas, even if performed on a computer.”); *Ashgari-Kamrani v. U.S. Servs. Auto. Ass’n*, No. 2:15-cv-

By contrast, the problem here arose because of computers, and the claims solve this technological problem by utilizing specialized computer technology. The only way Defendant is able to rebut this is by improperly generalizing the claims to erase their technical details. *See supra* § IV.A.3. This Court has previously rejected this approach. In *InsideSales.com*, the defendant also “cite[d] to many cases [] invalidating patents after the *Alice* decision.” 2017 WL 2559932, at *3. The Court rejected them because “these cases d[id] not involve the same kind of claimed technology.” *Id.* Like the cases Defendant cites here, “[c]ases involving patents that when stripped of computer or Internet jargon reveal a familiar business practice, not a technical solution to an Internet-centric problem or opportunity, are not particularly relevant.” *Id.*

This case is closer to *CosmoKey*. The patent there “recognize[d] that when a user communicates with a remote transaction partner (e.g., a bank, a store, or a secured database) via a communication channel like the Internet, ‘it is important to assure that an individual that identifies itself as an authorized user is actually the person it alleges to be.’” *CosmoKey*, 15 F.4th at 1093 (quoting U.S. Patent No. 9,246,903, at 1:30–46). “[I]nstead of requiring the user to input multiple authentication factors” via a “manual entry of information,” the patent disclosed an automatic process of “[c]hecking for an activated authentication function” so that “the user may activate the authentication function by activating their mobile device or by activating an application on a mobile device.” *Id.* at 1094 (citations omitted).

At *Alice* step one, the Federal Circuit noted it was “not convinced” by the defendant’s “broad characterization of the focus of the claimed advance,” similar to Defendant’s broad characterization of the claims here. *Id.* at 1097. At *Alice* step two, the Federal Circuit concluded

00478, 2016 WL 3670804 (E.D. Va. July 5, 2016) (“[T]he patent claims are directed to a common method for solving an old problem.”). Several of these decisions (both above and below the line) are also not precedential, and the Court is not bound to follow them.

that the “patent discloses a technical solution to a security problem in networks and computers,” even though the claims could be performed on conventional technology “of low complexity.” *Id.* at 1098. Like the claims here, the claims in *CosmoKey* “recite[d] a specific improvement to authentication that increases security.” *Id.* And, as here, “nothing in the specification or anywhere else in the record” suggests that the claimed steps “are conventional.” *Id.* To the contrary, the complaint and patent explain that these were novel ideas that solved a technological problem; indeed, that is why the USPTO issued the ’090 patent. Complaint ¶ 13.

D. If the Court Grants Defendant’s Motion, Dismissal Should Be Without Prejudice

If the Court grants Defendant’s motion to dismiss, then it should do so without prejudice and allow SAT to amend its complaint to include additional allegations showing the claims are directed to a technological solution. As Defendant explains in its motion, dismissal with prejudice is appropriate only if the intrinsic record “show[s] that the claim elements were well understood, routine, and conventional.” Mot. 23–24. Defendant has not pointed to anything in the patent that shows the process described in the claims was well-understood, routine, or conventional. All Defendant offers are conclusory statements that each step in isolation is “routine.” Mot. 4, 21. “Here, allowing [SAT] to file the proposed amended complaint, which alleges facts directed to the inventive concepts in its claimed invention, would not be futile.” *Aatrix*, 882 F.3d at 1126. Indeed, Defendant has not asserted that any potential amendment would be futile. The Court should therefore provide SAT leave to amend its complaint if the Court grants Defendant’s motion.

V. CONCLUSION

SAT respectfully asks the Court to deny Defendant’s motion to dismiss in view of well-pleaded facts that show the ’090 patent’s claims are eligible under 35 U.S.C. § 101.

Dated: October 2, 2025

/s/ Todd M. Briggs

Stephen Q. Wood (Utah Bar No. 12403)
stephenwood@quinnemanuel.com
2755 East Cottonwood Parkway, Suite 520
Salt Lake City, Utah 84121
Tel: (801) 515-7300
Fax: (801) 515-7400

Todd M. Briggs (*pro hac vice*)
toddbriggs@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, California 94065
Tel: (650) 801-5000
Fax: (650) 801-5100

Jonathan E. Pickhardt (*pro hac vice*)
jonpickhardt@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
295 5th Avenue, 9th Floor
New York, New York 10016
Tel: (212) 849-7000
Fax: (212) 849-7100

Christopher R. Sabbagh (*pro hac vice*)
chrissabbagh@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
700 Louisiana Street, Suite 3900
Houston, Texas 77002
Tel: (713) 221-7000
Fax: (713) 221-7200

*Attorneys for Plaintiff Secure Authentication
Technologies LLC*

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure, I hereby certify that, on October 2, 2025, all counsel of record who have appeared in this case are being served with a copy of the foregoing via CM/ECF.

Dated: October 2, 2025

/s/ Todd M. Briggs

Todd M. Briggs