

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

FRAUD FREE TRANSACTIONS LLC,

Plaintiff,

v.

PING IDENTITY CORPORATION,

Defendant.

C.A. No. 24-1218-GBW

Helena C. Rychlicki, Megan Ix Brison, PINCKNEY, WEIDINGER, URBAN & JOYCE LLC, Wilmington, DE; John S. LeRoy, Thomas A. Lewry, Sangeeta G. Shah, Reza Roghani Esfahani, BROOKS KUSHMAN P.C., Royal Oak, MI.

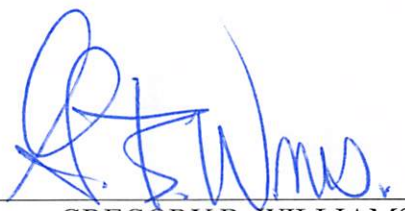
Counsel for Plaintiff

Kelly E. Farnan, RICHARDS, LAYTON & FINGER, P.A., Wilmington, DE; Orion Armon, COOLEY LLP, Denver, CO; Andrew Lau, COOLEY LLP, Palo Alto, CA; Rachel Preston, COOLEY LLP, Washington, D.C.

Counsel for Defendant

MEMORANDUM OPINION

April 29, 2025
Wilmington, Delaware


GREGORY B. WILLIAMS
UNITED STATES DISTRICT JUDGE

Pending before the Court is Defendant Ping Identity Corporation's ("Ping") Motion to Dismiss for Lack of Patent-Eligible Subject Matter (the "Motion") (D.I. 16), which has been fully briefed (D.I. 17; D.I. 20; D.I. 23). For the following reasons, the Court GRANTS Ping's Motion.

I. SUMMARY OF FACTS

Plaintiff Fraud Free Transactions LLC ("FFT") filed this action against Ping alleging that Ping infringes the Asserted Patents.¹ D.I. 1 (the "Complaint"). The '950 patent issued on September 17, 2024, and the '215 patent issued on January 10, 2023. Complaint ¶¶ 14-15. The Complaint asserts claims 1 and 2 of the '950 patent and claim 22 of the '215 patent. Complaint ¶¶ 27, 34.² Both patents are titled "Fraud Deterrence for Secure Transactions" and share a specification. Complaint ¶¶ 14-15.

The following factual allegations are taken as true for the purposes of this Motion. The Asserted Patents are "directed to specific and innovative approaches for securely permitting or denying users access to computer programs over a computer network." D.I. 20 at 2. In other words, these patents cover identity verification on a computer network. Verification of a user's identity over a computer network is more difficult than in-person verification. The increased difficulty results from the effective anonymity of the person using a computer network. Traditional user verification methods over a computer network, e.g., using a username and password, can have

¹ U.S. Patent Nos. 12,093,950 ("the '950 Patent") and 11,551,215 ("the '215 Patent").

² For purposes of this § 101 analysis, claims 1 and 2 are representative of all claims of the '950 patent and claim 22 is representative of all claims of the '215 patent. *See Sensormatic Elecs., LLC v. Wyze Labs, Inc.*, No. 2020-2320, 2021 WL 2944838, at *4 (Fed. Cir. July 14, 2021) ("Courts may treat a claim as representative in certain situations, such as if the patentee does not present any meaningful argument for the distinctive significance of any claim limitations not found in the representative claim." (citation omitted)).

less security issues because that information may be stolen and easily used by unauthorized individuals. D.I. 20 at 2.

A. The '950 Patent

The '950 Patent aims to address the flexibility and balance that effective security software must strike between providing enough security to prevent illicit access, while trying to keep procedures “simple” enough so as not to annoy legitimate users. D.I. 20 at 2. Prior art software security systems were rigid and frustrating to use because they did not consider the “context” of the request for access. *Id.* As recently as 2021, Ping’s competitor Okta said in one of its patents, “no identity product can be pre-defined to meet the requirement of supporting a variety of use cases with different contexts.” *Id.*

The invention in the '950 patent provides flexible, configurable rules that are applied based on the context of a request to access computer resources. *Id.* The invention determines the context based on the characteristics of the request, such as the origin of the request (digital or geographic) and whether the user is masking an IP address. *Id.* at 2-3. This method allows an organization to flexibly define rules unique to the organization’s operation that apply only if the organization’s disfavored markers are present. *Id.* at 3. By cascading the rules, each organization can determine the types of access attempts that are potentially fraudulent, and each organization can choose the nature of the tests and the levels of subsequent verification required. This approach improves over the prior art, which could not dynamically assess and respond to the “context” of user requests. *Id.*

Plaintiff asserts claims 1 and 2. Complaint ¶¶ 28-29. Claim 1 of the '950 patent claims a system that (1) receives an access request, (2) contains a set of rules to determine whether access should be granted that can be adjusted based on different situations, (3) where the rules include various checks to verify the identity of the user trying to access the software including things such

as the IP address, the geographic location of the user, or a device ID, and (4) depending on the results of the checks, the system can take different actions:

- (a) if everything is normal, the user can access the software without extra verification;
- (b) if something is unusual, additional identity verification may be required; and
- (c) if there is a risk of fraud, a more stringent verification process may be used.

Then, (5) the user can select the type of identity verification used for the required identity verification steps, and (6) the system grants access based on successful identity verification. *See* Complaint ¶ 28. In summary, Claim 1 is a system for adjusting identification requirements based on the risk associated with a request for access.

Claim 2 is dependent on claim 1 and recites that one of the risk-level determinations is based on comparing the originating IP address of the request to a designated IP address on file. Complaint ¶ 29.

B. The '215 Patent

The '215 patent covers a more secure technique for identity verification that ensures only a legitimate user can access restricted computer software. D.I. 20 at 3. Prior art methods used phone calls or text messages to provide “out of band” verification. Those methods were not fully secure because phone calls and texts can be sent by fraudsters masquerading as legitimate requests. The '215 patent attempts to solve that problem by employing a novel “fraud prevention application” on a mobile phone to prevent unauthorized access. Unlike the prior art that uses calls or texts, with the claimed invention, both the user and the service provider know the verification process is secure because both the confirmation request and response comes from a trusted application. *Id.*

Claim 22 depends on claim 21, which in turn depends on claim 20. Complaint ¶ 36. Independent claim 20 is directed to use of a dedicated “fraud prevention application” installed on

a “predefined” (i.e., trusted) “out-of-band” “mobile phone” that is “different” from the computing device a user is using to access a software application. Complaint ¶ 35. The users themselves authorize the request to access the software by using the fraud prevention application on a user’s mobile phone, which both the user and the software access provider know is a trusted application. Accordingly, the user knows the request comes from a source approved for communication with the application, and the provider knows the response is from a legitimate user. *Id.* The claims recite as follows:

Claim 20: A method of validating a request for access to software having a use restriction associated therewith, comprising:

receiving a request from an identified requestor for access to the software from a first computing device;

responsive to receiving the request, communicating with a fraud prevention application installed on a predefined out-of-band mobile phone, the mobile phone different from the first computing device and identified by a profile associated with the requestor;

obtaining approval or denial of the request from the application executing on the mobile phone;

determining whether the request was approved or denied based on a response from the application;

and responsive to the response indicating approval, processing the request to permit access to the software.

Claim 21: The method of claim 20, wherein the obtaining includes presenting, via the application executing on the mobile phone, a selectable option related to permitting the request.

Claim 22: The method of claim 21, wherein the presenting includes presenting a pop-up notification displayed to a user of the mobile phone.

Complaint ¶¶ 36-36. Each of these claims condition access to data or resources on: (1) initial evidence of identity, and (2) secondary evidence of identity.

II. JURISDICTION AND LEGAL STANDARDS

A. Jurisdiction

This Court has jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

B. Rule 12(b)(6) Motion to Dismiss

Federal Rule of Civil Procedure 8(a) requires that pleadings contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). “If pleadings fail to state a claim, in whole or in part, on which a court may grant relief, a defendant may seek to dismiss a complaint under Federal Rule of Civil Procedure 12(b)(6).” *Staton Techiya, LLC v. Harman Int’l Indus.*, 734 F. Supp. 3d 354, 363 (D. Del. 2024) (citing Fed. R. Civ. P. 12(b)(6)). “To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (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.* Plausibility requires “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* “In other words, a plausible claim must do more than merely allege entitlement to relief; it must support the grounds for that entitlement with sufficient factual content.” *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1352 (Fed. Cir. 2021) (citing *Iqbal*, 556 U.S. 662, 678). The Court assumes the factual allegations contained in the complaint to be true and draws all reasonable inferences in favor of the non-moving party when considering a motion to dismiss. *See Twombly*, 550 U.S. 544, 555-56. However, “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Iqbal*, 556 U.S. 662, 678.

The Federal Circuit applies regional circuit law to dismissals under Federal Rules of Civil Procedure 12(b)(6). *Glover v. Cohen*, No. 2021-2126, 2022 WL 5082130, at *2 (Fed. Cir. Oct. 5,

2022). Thus, “[t]he primary question in deciding a motion to dismiss is not whether the plaintiff will ultimately prevail, but rather whether they are entitled to offer evidence to establish the facts alleged in the complaint.” *Fenico v. City of Philadelphia*, 70 F.4th 151, 161 (3d Cir. 2023). In other words, “when a complaint adequately states a claim, it may not be dismissed based on a district court’s assessment that the plaintiff will fail to find evidentiary support for his allegations or prove his claim to the satisfaction of the factfinder.” *Twombly*, 550 U.S. at 563 n.8.

The Federal Circuit “ha[s] repeatedly recognized, ‘it is possible and proper to determine patent eligibility under 35 U.S.C. § 101 on a Rule 12(b)(6) motion.’” *Mobile Acuity Ltd. v. Blippar Ltd.*, 110 F.4th 1280, 1289-90 (Fed. Cir. 2024) (quoting *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369 (Fed. Cir. 2016)). “If patent eligibility is challenged in a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), [the court] must apply the well-settled Rule 12(b)(6) standard which is consistently applied in every area of law.” *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1357 (Fed. Cir. 2018). Patent eligibility under § 101 “can be determined at the Rule 12(b)(6) stage . . . only when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law.” *Beteiro, LLC v. DraftKings Inc.*, 104 F.4th 1350, 1355 (Fed. Cir. 2024) (quoting *Aatrix Software*, 882 F.3d at 1125).

C. Patent-Eligible Subject Matter

Patentability under 35 U.S.C. § 101 is a threshold legal issue. *Bilski v. Kappos*, 561 U.S. 593, 602 (2010). Section 101 of the Patent Act defines patent-eligible subject matter by stating “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” 35 U.S.C. § 101. The Supreme Court has held that there are exceptions to § 101. “Laws of nature, natural phenomena, and abstract ideas are not patentable.” *Alice Corp. Pty. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014) (internal

quotation marks and citation omitted). “[I]n applying the § 101 exception, [the Court] must distinguish between patents that claim the ‘building blocks’ of human ingenuity and those that integrate the building blocks into something more[] thereby ‘transforming’ them into a patent-eligible invention. The former ‘would risk disproportionately tying up the use of the underlying’ ideas and are therefore ineligible for patent protection. The latter pose no comparable risk of preemption, and therefore remain eligible for the monopoly granted under our patent laws.” *Id.* at 217 (cleaned up).

The Supreme Court’s *Alice* decision established a two-step framework for determining patent-eligibility under § 101. In the first step, the Court must determine whether the claims at issue are directed to a patent ineligible concept. *Id.* In other words, the Court asks whether the claims are directed to a law of nature, natural phenomenon, or abstract idea. *Id.* If the answer to the question is “no,” then the patent is not invalid for teaching ineligible subject matter under § 101. If the answer to the question is “yes,” then the Court proceeds to step two, where it considers “the elements of each claim both individually and as an ordered combination” to determine if there is an “inventive concept—i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.” *Id.* at 217-18 (alteration in original). “A claim that recites an abstract idea must include ‘additional features’ to ensure that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].” *Id.* at 221 (internal quotation marks and citation omitted). Further, “the prohibition against patenting abstract ideas cannot be circumvented by attempting to limit the use of [the idea] to a particular technological environment.” *Id.* at 222 (quoting *Bilski*, 561 U.S. at 610–11). Thus, “the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention.” *Id.* at 223.

III. DISCUSSION

The Court holds that, as a matter of law, the Asserted Patents are not directed to patent-eligible subject matter. First, the '950 patent fails the *Alice* test because it is directed to the abstract idea of adjusting identification requirements based on the risk associated with a transaction and otherwise lacks an inventive concept. Second, the '215 patent fails the *Alice* test because it is directed to the abstract idea of preventing fraud by requiring identity verification from multiple sources and otherwise lacks an inventive concept. Because these patents both fail the *Alice* test, they are not eligible under § 101.

A. The '950 Patent Claims are Invalid Under 35 U.S.C. § 101

Ping moves to dismiss Count I of the Complaint by asserting that the claims of the '950 patent are invalid under § 101. D.I. 17 at 6. Because the '950 patent claims are not directed to patent-eligible subject matter and lack an inventive concept, they fail both steps of the *Alice* test. Therefore, the Court grants Ping's motion to dismiss Count I of the Complaint.

1. *Alice* Step One: Claims 1 and 2 are Directed to an Abstract Idea

Claims 1 and 2 of the '950 patent fail step one of the *Alice* test because they are directed to an abstract idea. They are directed to the abstract idea of adjusting identification requirements based on the risk associated with a transaction. There are four basic steps: 1) receiving an access request, 2) applying a set of rules to evaluate the risk associated with the request, 3) selecting the number of authentication or identification verification steps based on risk level, and 4) then granting or denying access based on the results of the identification process.

The Federal Circuit has held that “analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, [is] essentially mental processes within the abstract-idea category.” *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016). Furthermore, courts look to “whether the claims in these patents focus on a specific

means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery.” *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016).

Ping analogizes the claims of the ’950 patent to how a high-security building manages visitor access. D.I. 17 at 7. First, the visitor requests entry into the building. Second, the building has a set of rules to determine the amount of identity verification steps based on the level of risk. For example, a more trusted visitor may only need to present an ID while a more unknown visitor may need to present an ID, sign in, and provide confirmation of an appointment. Third, the building applies verification steps for a given visitor. Fourth, the building will grant or deny access based on the results of the identity verification steps. D.I. 17 at 7.

Under *Alice* and its progeny, claims 1 and 2 are directed to abstract idea. First, the claims are simply a way to “analyz[e] information by steps people go through in their minds.” *Electric Power Group*, 830 F.3d at 1354. Crafting a system of rules for different levels of security risk is a process a person can go through in his or her mind. Second, there is nothing in these claims that point to a specific improvement in computer technology itself. The method is instead “directed to the result or effect that itself is the abstract idea and merely invoke[s]” a generic computer system. *McRO*, 837 F.3d at 1314.

Though these claims are implemented in a computer system, these claims still focus software-focused inquiries. For a claim implemented in the software context to be non-abstract, *Alice* step one turns on two inquiries: “(1) ‘whether the focus of the claimed advance is on a solution to ‘a problem specifically arising in the realm of computer networks’ or computers,” *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1293 (Fed. Cir. 2020) (quoting *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257-58 (Fed. Cir. 2014)); and (2) “whether the claim is properly

characterized as identifying a ‘specific’ improvement in computer capabilities or network functionality, rather than only claiming a desirable result or function.” *TecSec*, 978 F.3d at 1293 (quoting *Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1306 (Fed. Cir. 2020)). Generally, claims directed to generalized steps to be performed on a computer using conventional computer activity are not patent eligible. *Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017).

These inquiries additionally confirm that these claims are directed to an abstract idea. First, the claims are not directed to a solution specifically arising in the realm of computer networks. While the claims are implemented through technology, the claims are not directed to the solution of a technological problem. Instead, they are directed to a “general concept . . . through the use of conventional devices, without offering any technological means of effecting that concept.” *Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1262 (Fed. Cir. 2016).

Second, these claimed steps do not require a technical improvement that would constitute a technological improvement over generic computer systems. If the claim merely requires a functional result “but does not sufficiently describe how to achieve these results in a non-abstract way,” then it does not pass *Alice* step one. *Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017). Here, the claims do not describe any specific technological improvement to how these processes are to be performed. There is nothing in claim 1 that is directed to *how* to implement out-of-region broadcasting on a cellular telephone. Rather, the claim is drawn to the idea itself. *See Affinity Labs of Texas*, 838 F.3d at 1258.

Specifically parsing the claims, claim 1 includes the limitation that “at least one MFA [multi-factor authentication] actions includes a choice of a plurality of authentication actions to be undertaken by the user, including, definition of two or more different selectable MFA actions from

which the choice can be made[.]” ’950 patent at cl. 1. It is true that the specification describes this method as providing a “number of advantages over current practices”, and it also states that “it provides the client with a number of options for helping the seller to ensure that the client does not intend a fraudulent purchase” by allowing “the client to choose or configure alternative FFT options which the seller or bank is comfortable.” ’950 patent at 40:24-35. However, this description does not negate the fact that the claim involves nothing more than abstract mental processes.

In addition, claim 2 adds that one of the risk-level determinations is based on comparing the originating IP address of the request to a designated IP address it may have on file. This kind of determination is a well-known human process. For example, building security may cross-check a visitor’s identification against a database in order to verify the credential presented.

FFT asserts that these claims satisfy *Alice* step one because they solve “a problem specifically arising in the realm of computer networks’ or computers.” D.I. 20 at 5 (quoting *TecSec*, 978 F.3d at 1293). In particular, FFT states that the ’950 patent claims are patent eligible because “[i]mproving security” is “a non-abstract computer functionality improvement” that is patent eligible. D.I. 20 at 5 (quoting *TecSec*, 978 F.3d at 1294). FFT characterizes claim 1 as “directed to user authentication for secure access to computer software that deterministically uses adaptive, reactive, and flexible security rules based on the context of the present user access request.” D.I. 20 at 5.

FFT goes on to recite the three rule types described in claim 1: the first does not invoke multi-factor authentication (“MFA”) because the authentication “resulted in expected values;” the second action requires a MFA action where the determination “resulted in at least one unexpected value;” and the third requires yet another MFA action where a third determination “indicated

potential fraud” based on a risk value associated with certain “characteristics” of the request for software access. *Id.* at 6.

However, these arguments fail to show that the ’950 patent “solve[s] a problem specifically arising in the realm of computer networks or computers.” *TecSec*, 978 F.3d at 1293. While the patent claims may be using a computer to improve security, this result is different from improving *computer security*. Two cases help illustrate this difference. The patent claims in this case resemble those in *Ericsson Inc. v. TCL Communication Technology Holdings Limited*, 955 F.3d 1317 (2020). In *Ericsson*, the Federal Circuit held ineligible claims describing “a system and method for controlling access to a platform for a mobile terminal for a wireless telecommunications system.” *Id.* at 1325-26. Those claims, the court explained, “merely ma[de] generic functional recitations that requests are made and then granted.” *Id.* at 1328.

On the other hand, in *TecSec*, which FFT cites, the Federal Circuit upheld the district court’s ruling of patent eligibility under § 101 for claims that were directed to “improving a basic function of a computer data-distribution network, namely, network security.” 978 F.3d at 1296. The Federal Circuit held that the claims were patent eligible because they went “beyond” the abstract idea of mere multi-level security. *Id.* at 1295. The claims expressly required accessing an “object-oriented key manager” and specified uses of a “label” as well as encryption for the access management. *Id.* (internal citations omitted). Because of these express claim elements, the claims went beyond the abstract idea of managing access to objects using multiple levels of encryption. *Id.* The court concluded by saying that “although the patent involves multi-level security, that does not negate the conclusion that the patent is aimed at solving a particular problem of multicasting computer networks.” *Id.* at 1296.

The difference between these two cases is informative to the '950 patent claims. Unlike the claims in *TecSec*, the '950 patent claims do not go beyond the abstract idea of adjusting identification requirements based on the risk associated with a transaction. The claims in *TecSec* addressed computer security, but the '950 patent only attempts to improve general security with a computer. Moreover, in contrast to *TecSec*, the '950 patent claims fail to add any express claim elements that would allow the patent to be directed to a non-abstract idea. Meanwhile, both the claims in *Ericsson* and the '950 patent claims make “generic functional recitations,” so the claims do not go beyond an abstract idea.

FFT attempts to distinguish the cases that Ping cites. D.I. 20 at 11. But all FFT claims is that the '950 patent “claims a specific technique for verifying identity of the user.” *Id.* This argument is merely conclusory, and without support, it is unavailing. *See ECB USA, Inc. v. Savencia, S.A.*, No. CV 19-731-RGA, 2020 WL 5369076, at *4 (D. Del. Sept. 8, 2020) (“As a general prudential rule, courts only decide issues that are fairly and fully presented. Therefore, cursory arguments not fully developed by the parties are waived.”); *Purewick Corp. v. Sage Prods., LLC*, 666 F. Supp. 3d 419, 441 (D. Del. 2023) (“[A]rguments . . . not squarely argued[] are considered [forfeited].”) (some alterations in original).

FFT also asserts that the '950 patent claims are eligible because they “depart[ed] from prior art solutions.” D.I. 20 at 7. Specifically, FFT claims that the conventional approach forced all users into a singular authentication paradigm. In light of the claimed approach, FFT contends that administrators can now “tailor access by applying different security policies to different users” or situations. *Id.* (quoting *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1304 (Fed. Cir. 2018)).

But this argument runs into the same problem as contending that the '950 patent claims “solve a problem specifically arising in the realm of computer networks or computers.” *TecSec*,

978 F.3d at 1293. *Finjan* is a case where a patent claimed a security profile approach where the administrators could “tailor access by applying different security policies to different users or types of users.” 879 F.3d at 1304. However, as the Federal Circuit made clear, the question of patent eligibility was whether the patent constituted “an improvement in computer functionality.” *Id.* The court held that the claims were eligible because the patent solved the issue of protecting against “obfuscated code—known viruses that have been cosmetically modified to avoid detection by code-matching virus scans.” *Id.* (internal quotes omitted). This patent solved a computer specific issue whereas the ’950 patent does not.

FFT also points to *McRO* as a case where the Federal Circuit held the claims-at-issue were patent eligible because they were limited to rules with “specific, claimed features” that allowed “for the improvement realized by the invention.” *McRO*, 837 F.3d at 1313. Again, however, the Federal Circuit in *McRO* held that the claims-at-issue were directed to an improvement in computer functioning, but that kind of improvement is not present in the ’950 patent. *Id.* (“The specific, claimed features of these rules allow for the improvement realized by the invention.”).

Finally, FFT identifies Federal Circuit language that warns courts not to “overgeneralize claims in the § 101 analysis” and to avoid “high level of abstraction” that is “untethered from the language of the claims.” *TecSec*, 978 F.3d at 1293 (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016)). FFT states that transactions over computer networks have an inherently difficult challenge of verifying visually anonymous users where it is impossible to rely on the visual clues that are present in an in-person verification process. D.I. 20 at 10. Regardless of the difficulty of online verification vis-a-vis in-person verification, this Court’s analysis has followed the steps previous cases have followed, and the interpretation of these claims is that they are directed to an abstract idea.

2. *Alice* Step Two: Claims 1 and 2 Lack an Inventive Concept

Claims 1 and 2 of the '950 patent fail *Alice* step two because they lack an inventive concept. In other words, the claim does not include “‘additional features’ to ensure ‘that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].’” *Alice*, 573 U.S. at 221 (alterations in original) (quoting *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 77 (2012)). Once again, FFT merely restates the language of the patent in an attempt to make the claims patent eligible. FFT does not point to an inventive concept nor an “ordered combination” that adds an inventive concept to the patent’s abstract idea. See *Personalized Media Commc’ns, LLC v. Amazon.com, Inc.*, 161 F. Supp. 3d 325, 329 (D. Del. 2015), *aff’d sub nom. Personalized Media Commc’ns, L.L.C. v. Amazon.com Inc.*, 671 F. App’x 777 (Fed. Cir. 2016) (citing *Alice*, 573 U.S. at 217-18).

FFT also asserts that Ping incorrectly argues that the '950 patent claims are conventional. D.I. 20 at 12. According to FFT, the specification and the prosecution history of the '950 patent demonstrate that the claims are “non-conventional.” *Id.* But FFT misreads the case law. When a court has found that a patent’s claims are directed to an abstract idea, the court “must examine 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 (cleaned up). The question, then, is not if claims are conventional but if there is any inventive concept that can transform the already abstract idea into a patent-eligible method. See *Robocast, Inc. v. Netflix, Inc.*, No. CV 22-305-JLH-CJB, 2025 WL 580350, at *3 (D. Del. Feb. 21, 2025) (“Since ‘[n]one of the claims recite an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application of the abstract idea,’ . . . the asserted claims are unpatentable under 35 U.S.C. § 101.” (quoting *International Bus. Machines Corp. v. Zillow Group, Inc.*, 50 F.4th 1371,

1380 (Fed. Cir. 2022))). Thus, whether the claims are conventional is irrelevant to this *Alice* step two inquiry.

B. Claim 22 of the '215 Patent is Invalid Under 35 U.S.C. § 101

Ping moves to dismiss Count II of the Complaint by asserting that claim 22 of the '215 patent is invalid under § 101. D.I. 17 at 6. Because claim 22 of the '215 patent is not directed to patent-eligible subject matter and lacks an inventive concept, it fails both steps of the *Alice* test. Therefore, the Court grants Ping's motion to dismiss Count II of the Complaint.

1. *Alice* Step One: Claims 22 is Directed to an Abstract Idea

Claim 22 of the '215 patent fails step one of the *Alice* test because it is directed to an abstract idea. The abstract idea in claim 22 is preventing fraud by requiring identity verification from multiple sources. It is a method of (1) receiving a request for access to the software, (2) communicating with a fraud prevention application installed on a mobile phone, (3) the fraud prevention application on the mobile phone providing an option related to the request using a pop-up notification displayed on the phone, (4) determining if the request is approved or denied based on the response from the application, and (5) if approved, permitting access to the software.

This claim merely invokes generic processes and machinery to attempt to monopolize a longstanding method of organizing human activity. Here, that method is requiring identity verification from multiple sources to prevent fraud in business transactions. To find an abstract idea, a court can “compare claims at issue to those claims already found to be directed to an abstract idea in previous cases.” *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1334 (Fed. Cir. 2016). In this case, “controlling access . . . or limiting permission to, resources” is abstract because “[c]ontrolling access to resources is exactly the sort of process that ‘can be performed in the human mind, or by a human using a pen and paper,’ which [courts] have repeatedly found unpatentable.”

Ericsson, 955 F.3d at 1326-27 (quoting *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011)).

Indeed, courts have routinely confirmed this method of controlling resources is abstract.³ The most relevant case is *Universal Secure Registry LLC vs. Apple Inc.*, 10 F.4th 1342 (Fed. Cir. 2021). In that case, the patent-at-issue had claims for an invention that required identity verification from multiple sources. *Id.* at 1351. The Federal Circuit explained that “verifying the identity of a user to facilitate a transaction is a fundamental economic practice that has been performed well before . . . computers and Internet transactions.” *Id.* at 1353 (quoting *Elec. Commun. Techs., LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1182 (Fed. Cir. 2020)). As a result, those claims recited “conventional actions in a generic way” without “improv[ing] any underlying technology.” *Universal Secure Registry*, 10 F.4th at 1352 (quoting *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1168 (Fed. Cir. 2019)).

Claim 22 of the ’215 patent is directed to the same abstract idea. Like the claims in *Universal Secure Registry*, restricting access to resources using multi-step authentication is an abstract idea. Furthermore, claim 22 does nothing to improve computer functionality. *See Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241 (Fed. Cir. 2016) (at *Alice* step 1, the court must “determine whether the claims focus on a specific means or method that improves the relevant

³ *Asghari-Kamrani v. United Servs. Auto. Ass’n*, No. 15-478, 2016 WL 3670804, at *5-6 (E.D. Va. July 5, 2016), *aff’d*, 737 F. App’x 539 (Fed. Cir. 2018) (affirming the district court’s ruling that a patent related to a method of multi-factor authentication using different communication mediums was invalid); *Smartflash, LLC v. Apple Inc.*, 680 F. App’x 977, 978-83 (Fed. Cir. 2017) (finding claims for conditioning access to data on verification of payment likewise to be directed to the abstract idea of “conditioning and controlling access to data”); *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App’x 1014, 1017 (Fed. Cir. 2017) (finding patent directed to the abstract idea of “providing restricted access to resources” ineligible for patenting); *In re AuthWallet, LLC*, No. 2022-1842, 2023 WL 3330298, at *3 (Fed. Cir. May 10, 2023) (finding claims “directed to a method for processing financial transaction data that implements authorization requests” to be an abstract idea).

technology or are directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery.” (cleaned up)). Both the claims in *Universal Secure Registry* and claim 22 of the ’215 patent rely on generic computer technologies to carry out an abstract idea. As a result, claim 22 is directed to an abstract idea.

FFT asserts that claim 22 satisfies *Alice* step one because it provides a technological improvement such that it improves computer security and remote authentication over the Internet. D.I. 20 at 13. According to FFT, prior to the ’215 patent, remote authentication over the Internet lacked a trusted fraud prevention application on a user’s phone that could be used to secure access to an application from a different computing device. *Id.* Under FFT’s theory, the ’215 patent increased security by involving active participation of “both the authorized user and the software/service provider in a process that certifies the phone as approved for use in this verification.” D.I. 20 at 13.

However, FFT provides no textual support for a technological improvement. Instead, FFT merely provides conclusory quotes from the ’215 patent and claims those quotes show a technological improvement. For example, FFT pulls language from the ’215 patent specification to claim that the installation of the fraud prevention application is “simpl[i]fied” and yet “very effective.” D.I. 20 at 14 (quoting D.I. 1-1, ’215 Patent, 17:22-25). Furthermore, FFT provides the language from the Notice of Allowance from the ’215 Patent prosecution history which states that the claimed method “provides a specific improvement over prior systems.” *Id.* at 15 (quoting Ex. 4, Notice of Allowance, at ¶ 15.⁴ But providing these conclusory statements without

⁴ Ping makes an argument that “FFT improperly relies on extrinsic evidence” when it quotes the prosecution history and the Declaration of Paul D Martin, PhD. D.I. 23 at 1. That argument does not affect the outcome of this motion for three reasons. First, under a Rule 12(b)(6) motion, a court must take “all plausible factual allegations in the complaint as true and constru[e] those factual allegations in the light most favorable to the non-movant.” *Conti v. U.S.*, No. 2024-1403,

underlying support does not persuade this Court. *See ECB USA*, 2020 WL 5369076, at *4 (“As a general prudential rule, courts only decide issues that are fairly and fully presented. Therefore, cursory arguments not fully developed by the parties are waived.”); *Purewick Corp.*, 666 F. Supp. 3d at 441 (D. Del. 2023) (“[A]rguments . . . not squarely argued[] are considered [forfeited].”) (some alterations in original).

Finally, FFT contends that Ping lacks support from caselaw for this Motion while also mischaracterizing the claimed invention. D.I. 20 at 16. That contention is incorrect. Ping has provided many cases that this Court can look to for finding an abstract idea. *See supra* n.3. And FFT’s attempts to distinguish these cases fail. Further, FFT stresses that the ’215 patent requires a “fraud prevention application,” which the previously cited cases do not. *Id.* at 17. But FFT cannot circumvent the “prohibition against patenting abstract ideas . . . by attempting to limit the use of [the idea] to a particular technological environment.” *Alice*, 573 U.S. at 222 (alteration in original) (citation omitted). The fact that the ’215 patent has “a specific need for implementation by computers” does not mean that Ping’s cited cases are inapposite. *Id.*⁵

2024 WL 4100410, at *3 (Fed. Cir. Sept. 6, 2024). Second, the Court considers only the facts in the complaint and the Asserted Patents. *See Aatrix Software*, 882 F.3d at 1128 (“[T]he sources properly considered on a motion to dismiss [include] the complaint [and] the patent.”). The Court is able to resolve this Motion with those facts alone. Third, the cases that Ping cites favor the non-movant party wherein the courts deferred the motion to dismiss to a later stage of the litigation. This Court assumes that that result is not the preferred outcome for Ping.

⁵ FFT also mischaracterizes the reason why the Federal Circuit held the claims-at-issue ineligible in *Universal Secure Registry*, 10 F.4th. FFT asserts the claims were ineligible because they were “conventional.” D.I. 20 at 17. As this Court has explained *supra*, the claimed patented method in *Universal Secure Registry* was a “fundamental economic practice” that did not “improv[e] any underlying technology.” *Id.* at 1352.

2. *Alice* Step Two: Claim 22 of the '215 Patent Lacks an Inventive Concept

Claim 22 of the '215 patent fails *Alice* step two because it lacks an inventive concept. Instead, the claim does no more than apply the abstract idea “with a computer.” *Alice*, 573 U.S. at 223. Additionally, the steps of claim 22, whether considered alone or in combination, invoke “well-understood, routine, [and] conventional” technology to carry out the abstract idea. *Id.* at 225 (quoting *Mayo*, 566 U.S. at 79).

For example, the claimed steps of “receiving” and “obtaining” authentication lists only generic components of “mobile phone” and “computing device” that merely execute the abstract idea. Complaint ¶ 35. As another example, the “out-of-band mobile phone” was a method that existed before this patent issued. *See StrikeForce Techs., Inc. v. SecureAuth Corp.*, No. 17-04314-JAK-SK, 2017 WL 8808122, at *6 (C.D. Cal. Dec. 1, 2017), *aff'd*, 753 F. App'x 914 (Fed. Cir. 2019) (finding the use of out-of-band authentication to be “familiar processes in the context of the use of computers that are connected to the internet.”). Finally, the recitation of the phrase “fraud prevention application” does not add an inventive concept because, like the previous two examples, “conventional generic computer components employed in a customary manner” is “insufficient to transform [an] abstract idea into a patent-eligible invention.” *Elec. Power*, 830 F.3d at 1354.

Importantly, improved speed or efficiency does not necessarily mean a patented method is a technological improvement and, thus, patent eligible. *See Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Canada*, 687 F.3d 1266, 1278 (Fed. Cir. 2012) (“[T]he fact that the required calculations could be performed more efficiently via a computer does not materially alter the patent eligibility of the claimed subject matter.”); *CLS Bank, Int'l v. Alice Corp.*, 717 F.3d 1269, 1286 (Fed. Cir. 2013) (en banc) (“[S]imply appending generic computer functionality to lend speed or efficiency to the performance of an otherwise abstract concept does not meaningfully limit claim

scope for purposes of patent eligibility.”), *aff’d*, 573 U.S. 208 (2014). This rule comports with the underlying logic of the *Alice* test: that taking an abstract idea and having a computer run it (which is often faster than humans) does not mean it is a technological improvement. *Alice*, 573 U.S. at 222 (“The introduction of a computer into the claims does not alter the analysis at . . . step two”).

FFT claims that this patent passes *Alice* step two because Ping does not point to any case that holds that a “fraud prevention application on a specific mobile device” is ineligible. D.I. 20 at 18. In support, FFT cites *CosmoKey Solutions GmbH & Co. v. Duo Security LLC*, 15 F.4th 1091 (Fed. Cir 2021). There, the Federal Circuit ruled that there was an inventive concept at *Alice* step two because of a specific improvement. That improvement, the Federal Circuit explained, prevented unauthorized access by a third party, even though “authentication of a user’s identity using two communication channels and a mobile phone was known.” *Id.* at 1098. Because the Federal Circuit found an inventive concept there, FFT contends the Court must find a specific improvement and a corresponding inventive concept in claim 22 of the ’215 patent. D.I. 20 at 19.

FFT’s argument, however, fails because it ignores the reason for the Federal Circuit’s holding in *CosmoKey*. In that case, the Federal Circuit found that using a timing-based approach enhanced security and, thus, provided a specific improvement in authentication. The Federal Circuit highlighted how the specification of the patent at issue performed “user authentication with fewer resources, less user interaction, and simpler devices.” *CosmoKey*, 15 F.4th at 1099. These facts were enough for a finding of improved computer functionality. *Id.* at 1098. Here, however, FFT does not provide any support of claim 22 of the ’215 patent improving computer function.

FFT concludes its argument by claiming that Ping has not offered evidence that claim 22 of the ’215 patent invokes well-understood, routine, and conventional technology to the carry out the abstract idea. D.I. 20 at 20. However, in its brief, Ping sufficiently sets forth the reasons that

claim 22 of the '215 patent fails *Alice* step 2 because the claim—whether considered alone or in combination—invokes “well-understood, routine, [and] conventional” technology to carry out the abstract idea, D.I. 17 at 17 (citing *Alice*, 573 U.S. at 225), “the '215 specification does not disclose any specific improvement to these conventional, well-understood, and routine techniques,” and “nothing about the ‘ordered combination’ of claim elements ‘transforms’ the nature of the claims into a patent-eligible invention.” D.I. 17 at 17-19 (quoting *Alice*, 573 U.S. at 217). Ping also has cited appropriate cases to support its argument. *See id.*

IV. CONCLUSION

For the foregoing reasons, the Court grants Defendant’s Motion. An Order consistent with this Memorandum Opinion will be entered.

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

FRAUD FREE TRANSACTIONS LLC,

Plaintiff,

v.

PING IDENTITY CORPORATION,

Defendant.

C.A. No. 24-1218-GBW

ORDER

At Wilmington this 29th day of April, 2025, consistent with the corresponding Memorandum Opinion, **IT IS HEREBY ORDERED** that Defendant Ping Identity Corporation's Motion to Dismiss for Lack of Patent-Eligible Subject Matter (D.I. 16) is **GRANTED**.



GREGORY B. WILLIAMS
UNITED STATES DISTRICT JUDGE