No. 21-____

IN THE

Supreme Court of the United States

UNIVERSAL SECURE REGISTRY LLC,

Petitioner,

v.

APPLE INC., VISA INC., VISA U.S.A. INC.,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Federal Circuit

PETITION FOR A WRIT OF CERTIORARI

KEVIN A. SMITH
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California St.
22nd Floor
San Francisco, CA 94111
(415) 875-6600

KATHLEEN M. SULLIVAN
Counsel of Record
TIGRAN GULEDJIAN
CHRISTOPHER MATHEWS
QUINN EMANUEL URQUHART & SULLIVAN, LLP
865 South Figueroa St.
10th Floor
Los Angeles, CA 90017
(213) 443-3000
kathleensullivan@quinnemanuel.com

Counsel for Petitioner

January 27, 2022

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

QUESTION PRESENTED

Section 101 of the Patent Act provides that "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof," is eligible for a patent. 35 U.S.C. § 101. The question presented is:

Does patent eligibility under 35 U.S.C. § 101 require "specificity," "unexpected results" and "unconventionality," in conflict with the Patent Act and this Court's decision in *Alice Corp. Pty. Ltd.* v. *CLS Bank International*, 573 U.S. 208 (2014)?

PARTIES TO THE PROCEEDINGS BELOW

Petitioner Universal Secure Registry LLC was plaintiff-appellant below.

Respondent Apple Inc. was defendant-appellee below.

Respondent Visa Inc. was defendant-appellee below.

Respondent Visa U.S.A. Inc. was defendant-appellee below.

RULE 29.6 STATEMENT

KW Strategic Enterprises, LLC owns 10 percent or more of the stock of Universal Secure Registry LLC.

RELATED PROCEEDINGS

Universal Secure Registry LLC v. Apple Inc., No. 1:17-cv-585 (D. Del.)

Universal Secure Registry LLC v. Apple Inc., No. 20-2044 (Fed. Cir.)

TABLE OF CONTENTS

APPENDIX

TABLE OF AUTHORITIES

Page(s)

United States Supreme Court Cases

Federal Circuit Court Cases

Federal Statutory Authorities

Federal Rules and Regulations

Legislative Materials

Additional Authorities

INTRODUCTION

This petition arises from a decision of the Federal Circuit that invalidated the claims of four patents under 35 U.S.C. § 101 on the ground that they claim only an abstract idea. The Federal Circuit so ruled even though the inventions provide a new and useful process for securely authenticating user-merchant transactions with a simple click, touch, or biometric input on mobile devices.

The decision thus continues a concerning pattern in which the Federal Circuit issues inconsistent and unpredictable section 101 decisions in an effort to apply this Court's decision in *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). That pattern has caused grave uncertainy among inventors and patent practitioners and so destabilized the patent system that the active Federal Circuit judges "are at a loss as to how to uniformly apply § 101" and have made a "unanimous [and] unprecedented plea for guidance." *American Axle & Mfg., Inc. v. Neapco Holdings LLC*, 977 F.3d 1379, 1382 (Fed. Cir. 2020) (Moore, J., concurring), *cert. pending* (No. 20-891). That plea has been echoed by calls to this Court from legislators, former directors of the USPTO, the Solicitor General and others to clarify the *Alice* test. This case presents an ideal opportunity to provide that needed guidance.

Alice articulated a two-step test for determining whether an invention is ineligible for patenting pursuant to section 101. The first step requires a court to determine if the patent claim is directed to a patent-ineligible concept, such as an abstract idea. 573 U.S. at 218. If the answer to this initial determination is "yes," then the second step requires

the court to consider whether the claim elements contain an "inventive concept" sufficient to "transform the nature of the claim into a patent-eligible application." *Id.* at 221 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72-73, 78-79 (2012)) (quotation marks omitted). *Alice* did not, however, articulate a methodology to determine, at step one, whether a patent claim is "directed to an abstract idea" and, if so, what that abstract idea is. Instead, this Court stated that it "need not labor to delimit the precise contours of the 'abstract ideas' category," *Alice*, 573 U.S. at 221, leaving that task for a later case.

This is the perfect case in which to do so. The opinion below conflicts with both this Court's precedent and the Patent Act in four separate ways. *First*, the Federal Circuit grafted a "specificity" requirement onto *Alice*. *Second*, the court required a showing of "unexpected results," contrary to *Alice* and *Diamond v. Diehr*, 450 U.S. 175 (1981). *Third*, it required proof, as part of *Alice* step one, that the claim was "unconventional," even though unconventionality only comes into play under *Alice* at step two. *Finally*, the court held that the claims failed step two for essentially the same reasons they failed step one, effectively collapsing *Alice*'s two-step test into a single step.

Because the Federal Circuit's decision conflicts with *Alice, Diehr*, and the Patent Act, it warrants review so that the Court can clarify the *Alice* step-one standard. In the alternative, this Court should hold this petition pending the Court's disposition of *American Axle & Manufacturing, Inc. v. Neapco*

Holdings LLC, No. 20-891, in which this Court has called for the views of the Solicitor General.

OPINIONS BELOW

The opinion of the U.S. Court of Appeals for the Federal Circuit is reported at 10 F.4th 1342 and is reproduced at App. 1a. The district court's opinion is reported at 469 F. Supp. 3d 231 and reproduced at App. 31a.

JURISDICTION

The court of appeals denied rehearing on October 29, 2021. App. 78a. This Court has jurisdiction under 28 U.S.C. § 1254(1).

PERTINENT STATUTORY PROVISIONS

35 U.S.C. § 101 states: "Whoever 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. § 112(b) states: "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention."

STATEMENT OF THE CASE

A. Statutory Background

The Patent Act, 35 U.S.C. § 101, provides that "[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." Other sections of the Patent Act separately require that, apart from being "new and useful," a patent must be novel, nonobvious, and particularly described. 35 U.S.C. §§ 102, 103, 112.

B. Factual Background

Dr. Kenneth P. Weiss, an expert in the fields of information systems security and multifactor identity authentication, is the founder of Universal Secure Registry LLC ("USR"). Before starting USR, Dr. Weiss founded and served for many years as the CTO and Chairman of the Board of Security Dynamics Technologies Inc., now RSA Security LLC. At Security Dynamics, Dr. Weiss invented SecurID tokens and their underlying algorithm that became a leading form of personal identity authentication for computer security and electronic commerce. Dr. Weiss's SecurID technology is being used by more than 150 million people, more than 90% of Fortune 500 companies, and corporations, consumers, governments, and banks in more than thirty countries. His technology has been used by all three branches of the United States government, including the Department of Defense, the Treasury, the Senate, and the White House.

Dr. Weiss has also developed technological solutions for identity authentication, computer security, and digital and mobile payment security for USR. His innovations allow users to securely authenticate their identity using technology built into a personal electronic device combined with the user's own secret or biometric information. Such authentication is secure, useful, and convenient across a variety of contexts.

Dr. Weiss's work resulted in the issuance of patents to USR related to securing electronic payment transactions, four of which are at issue here. App. 2a. Although electronic payment transactions are commonplace, they can expose one's sensitive financial or personal information to bad actors. Before the claimed inventions, customers used their credit cards at a merchant's in-store point-of-sale device, which would read the card number and other account data from the magnetic stripe or chip on the card. Magnetic-stripe technology, however, had disadvantages. In addition to requiring a magnetic-stripe-reader device, magnetic-stripe technology lacked adequate security and was susceptible to fraud. Magnetic-stripe-reader systems also typically required customers to provide their credit card account data (and sometimes personal information such as address, telephone number, or zip code) directly to online merchants, who would store the account data and transmit it through a network to the card's issuing bank for transaction approval (or disapproval). When a person paid a merchant by credit card, the account data was exposed to the risk of misuse by the merchant or a bad actor who intercepted the data as it was sent over a network to the merchant or the credit card company. App. 3a, 9a, 15a, 20a-21a, 24a-25a.

USR's patents address the need for technology that allows consumers to conveniently make payment-card transactions without a magnetic-stripe reader and with a high degree of security. USR's inventions enable users to conduct secure transactions with a simple click, touch, or biometric input on their personal hand-held devices, enabling contactless transactions that are authenticated by

multiple factors. The user never has to hand a card to a third person or come in contact with point-of-sale hardware that belongs to the merchant. The user device does not store or send any sensitive information, such as personal account information or payment card details, that, if compromised, could be used for fraudulent purposes. Instead, the user device locally generates and wirelessly sends data, including a single-use cryptographic value, used for authentication. App. 9a, 15a, 20a-21a, 24a-25a. A new cryptographic value is generated each time a transaction occurs, and the value is verified by the payment processor before the transaction is approved. App. 9a, 15a, 21a. The user device can also require the user to authenticate him or herself via entry of secret information (e.g., a PIN) and/or biometric information (e.g., a fingerprint) before the user device will carry out a payment. App. 15a, 18a-20a, 35a. As a result, even if the user device is lost or stolen or the one-time cryptographic value is intercepted, neither the user device nor the value can be used to make a fraudulent purchase.

USR's inventions not only provide novel and improved ways of authenticating users for the purpose of electronic payments, but also reshape the technology of prior payment-processing systems themselves. For example, the inventions reduce the need for the network to include the use of magnetic-stripe-reading devices, the need to transmit sensitive identifying or financial information to untrusted merchant servers, the need for a secured communication connection, and the need for the user to carry forms of physical identification. App.8a.

Recognizing the promise of these inventions, Dr. Weiss and USR sought to partner with Apple and Visa to commercially develop this technology. To that end, Dr. Weiss and USR disclosed the technology to Apple in several letters, presented it to Visa, and proposed jointly developing a product. Neither Apple nor Visa partnered with USR, however, choosing instead to partner with each other to incorporate the technology into their Apple Pay and Visa Token Service products.

C. USR's Complaint

Upon learning of Apple's and Visa's unauthorized use of the technology, USR filed a complaint in the District of Delaware alleging infringement of four patents: U.S. Patent Nos. 8,856,539 ("the '539 patent"); 8,577,813 ("the '813 patent"); 9,100,826 (the '826 patent"); and 9,530,137 ("the '137 patent"). C.A.Appx7-Appx243. The patents claim related but distinct computer authentication inventions designed to protect users' personal and financial information.

Claim 22 of the '539 patent is illustrative. It describes an anonymous identification system that allows verification without requiring the user to expose personal information. For example, it allows the purchase of goods without providing credit card information to the merchant, thereby preventing the information from being stolen or used fraudulently. Claim 22 states:

> 22. A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity

> is identified by a time-varying multi character code, the method comprising:
>
> receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;
>
> mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;
>
> determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;
>
> accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;
>
> providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction; and
>
> enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information.

App. 9a-10a.

The '813 patent also allows users to securely authenticate their identity when making a credit

card transaction. To perform this authentication, an electronic ID device generates a non-predictable value (*e.g.*, a random number) using, for example, the user's biometric information. App. 15a-16a. The device generates single-use authentication information using the nonpredictable value, information associated with the user's biometric data (e.g., a fingerprint), and the user's secret information (e.g., a PIN), which is transmitted to a secure registry for authentication. App. 15a-16a.

The '826 patent similarly authenticates a user's identity, first by using biometric information, and second based on authentication information (*e.g.*, a variable one-time token) determined from the user's biometric information. App. 20a-21a. The system provides additional security by relying on encrypted authentication information generated using a time-varying non-predictable signal from the biometric information. App. 20a-21a.

Finally, the '137 patent describes a related transaction-approval system. The user's identity must be authenticated based on his secret information and biometric information. The device generates authentication information, an indicator of the biometric authentication of the user, and a time-varying value that creates a one-time variable token that can be sent via a merchant to a second device for transaction approval. App. 25a-26a.

D. Related PTAB Proceedings

In response to USR's complaint, Apple and Visa filed several petitions in the Patent Trial and Appeal Board ("PTAB") for *inter partes* and covered business method review of USR's patents. In particular,

Apple sought covered business method review of the '813 patent on the ground that its claims were allegedly unpatentable under 35 U.S.C. § 101.

Applying the two-step analysis set forth in *Alice*, the PTAB declined to institute that proceeding, concluding that Apple failed to show that it is more likely than not that any claim was unpatentable. Specifically, the PTAB concluded that the claims were not directed to an abstract idea. Instead, the PTAB reasoned:

> A reading of the challenged claims reveals they require more than simply verifying an account holder's identity based on codes or account holder information as alleged by Petitioner. Rather, we find that these claims are directed to an improvement in the security of mobile devices by using a biometric sensor, a user interface, a communication interface, and a processor working together to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be used fraudulently in subsequent transactions.

C.A. Appx5266.

E. District Court Proceedings

Despite the PTAB's ruling, Apple and Visa moved in the district court to dismiss USR's complaint for failure to state a claim, arguing again that the patents claimed unpatentable subject matter under 35 U.S.C. § 101. The court referred the motion to the magistrate judge for a report and recommendation.

After briefing and oral argument, the magistrate issued a report and recommendation concluding that none of the claims was directed to an abstract idea under *Alice* step one and therefore recommending that the district court deny the motion to dismiss. App. 48a. Specifically, the magistrate judge found that, because "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity," the patents claimed patentable inventions. App. 67a, 69a, 71a, 73a.

Apple and Visa filed objections to the magistrate's report and recommendation. In its ruling on those objections, the district court disagreed with the magistrate's analysis and held that the exemplary claims were unpatentable under 35 U.S.C. § 101. The district court ruled that, under *Alice* step one, each claim was directed to an abstract idea, which the court variously characterized, depending on the patent, as "the secure verification of a person's identity," App. 40a, "a method to obtain the secure verification of a person's identity to enable a commercial transaction," App. 41a, "obtaining the secure verification of a user's identity to enable a transaction," App. 42a, "secured verification of a person's identity," App. 44a, "authenticating identity," App. 46a, or a "system for authenticating a user for enabling a transaction," App 46a-47a.

Unlike the magistrate judge, who had no need to reach *Alice* step two in light of her finding that each claim survived step one, the district court concluded at step two that none of the claims involved an inventive concept, asserting in conclusory language that the patents' inventions merely taught the use of

"conventional" or "generic" computer and other device components. App. 42a-47a. The district court, therefore, dismissed the complaint for failure to state a claim for relief.

F. The Court Of Appeals Opinion

USR appealed to the Federal Circuit. It argued in part that the district court erred in concluding that the claims were directed to abstract ideas under *Alice* step one. In a published opinion, the court affirmed the judgment. App. 1a-30a; 10 F.4th 1342. The opinion began by applying a technology-specific patent eligibility rule of its own devising, namely that, "[i]n cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." App. 5a-6a. The opinion then concluded that all claims failed both of *Alice*'s two steps.

At step one, the court held that each claim is directed to an abstract idea. Although the patents and their claims differ, the Federal Circuit's reasoning for each was similar, holding that they were directed to abstract ideas because they allegedly lacked specificity, failed to produce unexpected results, or recited conventional limitations. App. 12a-13a, 17a-18a, 22a-23a, 27a-28a. The court concluded (with little explanation how it derived these varying "abstract ideas") that the claims were directed to "a method for enabling a transaction between a user and a merchant, where the merchant is given a time-varying code instead of the user's secure (credit card) information," App. 11a-12a, "a method for verifying the identity of a user to facilitate an economic transaction," App. 13a,

"an electronic ID device that includes a biometric sensor, user interface, communication interface, and processor working together to (1) authenticate the user based on two factors—biometric information and secret information known to the user—and (2) generate encrypted authentication information to send to the secure registry through a point-of-sale device," App. 17a, "collecting and examining data to enable authentication," App. 18a, and "multi-factor authentication of a user's identify using two devices to enable the transaction," App. 22a, 26a.

The court then held that each claim also failed step two for substantially the same reasons they failed step one. The court began its step-two analysis by cross-referencing its step-one reasoning. App. 18a-19a, 29a. The court then held that the claims failed step two for essentially the same reasons as step one, namely their limitations were allegedly "conventional," "nonspecific," and yielded only "expected results" without "unexpected improvement." App. 13a, 18a-20a, 23a-24a, 29a-30a.

USR petitioned for panel rehearing and rehearing en banc, arguing that the decision conflicted with this Court's *Alice* two-step test for eligiblity. In particular, USR explained that the opinion deviated from this Court's precedent by imposing a heightened "specificity" requirement for authentication patents, by requiring that the patent produced "unexpected results" and "unconventionality" to satisfy *Alice*'s step one, and by collapsing the test's two distinct steps into one by applying the same analysis at both steps. On October 29, 2021, the court denied that petition for rehearing. App. 79a.

REASONS FOR GRANTING THE WRIT

I. The Decision Below Warrants Review

"Whoever 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. Congress drafted this provision "in broad terms to fulfill the constitutional and statutory goal of promoting 'the Progress of Science and the useful Arts.'" *Diamond v. Chakrabarty,* 447 U.S. 303, 315 (1980). This Court has recognized "three specific exceptions to § 101's broad patent-eligibility principles: 'laws of nature, physical phenomena, and abstract ideas.'" *Bilski v. Kappos,* 561 U.S. 593, 601 (2010) (quoting *Chakrabarty,* 447 U.S. at 309).

In *Alice*, this Court set forth a two-step test to distinguish between patent-eligible subject matter and these patent-ineligible judicial exceptions. The first step requires determining whether a patent claim is "directed to one of [the] patent-ineligible concepts" such as an abstract idea. 573 U.S. at 217-18. If the answer to this initial determination is "yes," then the second step asks whether the claim elements contain an "inventive concept" sufficient to "transform the nature of the claim into a patent-eligible application." *Id.* at 217 (quoting *Mayo,* 566 U.S. at 72-73,79 (quotation marks omitted)). To be patent-eligible, the "inventive concept" must be "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 (quoting *Mayo*, 566 U.S. at 72-73 (cleaned up)).

Notably, however, *Alice* failed to articulate a standard or methodology to determine, at step one, whether a patent claim is "directed to an abstract idea" and, if so, what that abstract idea is. Instead, this Court stated that it "need not labor to delimit the precise contours of the 'abstract ideas' category." *Alice*, 573 U.S. at 221; *see Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1334 (Fed. Cir. 2016) ("The Supreme Court has not established a definitive rule to determine what constitutes an 'abstract idea' sufficient to satisfy the first step of the *Mayo/Alice* inquiry."). *Alice* left that task for a later case. Since that decision and in the absence of this Court's guidance, the Federal Circuit has struggled to consistently apply *Alice* step one.

A. The Decision Below Conflicts With *Alice* And The Patent Act

The decision below contravenes *Alice* in four respects that warrant this Court's review. Review is needed to resolve those conflicts and dispel the Federal Circuit's confusion regarding the first step of *Alice*'s test for patent eligibility. *First*, the Federal Circuit imposed a "specificity" requirement of its own creation. *Second*, the court adopted a novel "unexpected results" test. *Third*, it required proof of "unconventionality" as part of step one, even though, under *Alice*, a showing of conventionality is relevant only to step two. *Finally*, at *Alice* step two, the court cross-referenced its step-one analysis and held that the claims failed step two for the same reasons, effectively collapsing *Alice*'s two-step test into a single step.

1. The Federal Circuit's "Specificity" Test Is Contrary To *Alice*

The Federal Circuit held that USR's patent claims failed *Alice* step one due in part to a purported lack of specificity. App. 17a, 22a-24a, 27a. In particular, the court announced a technology-specific rule of its own devising that, "[i]n cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." App. 5a-6a. The court then held that three of the patents failed *Alice* step one under this test because: (1) the '813 patent claims lack "a specific technical solution by which the biometric information or the secret information is generated, or by which the authentication information is generated and transmitted," App. 17a; (2) the '826 patent "claims do not include sufficient specificity" and did not recite a "a specific technical solution," App. 22a; and (3) the '137 patent claims "are not sufficiently specific," App. 27a.

This Court should grant certiorari to clarify that step one does not include a specificity test. *Alice* does not purport to apply a "specificity" test. *See Alice*, 573 U.S. at 218-21. The authority cited by the Federal Circuit for this "specificity" requirement was limited to its own prior decisions, none of which derives that test from this Court's precedent. *See* App. 5a-8a.[1]

---

[1] The Federal Circuit has, in other cases, announced a specificity requirement at *Alice* step one for "[c]aims to the genus of an invention, rather than a particular species." *McRO,*

The Federal Circuit's "specificity" requirement cannot be found in or implied from the text of § 101. Claim specificity is, instead, governed by 35 U.S.C. § 112(b), which requires patent claims to be "particular[]" and "distinct[]," not by § 101. Section 112(b) has its own well-developed jurisprudence. *See Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014) (interpreting § 112(b) to require that a patent claim be specific enough "to inform those skilled in the art about the scope of the invention with reasonable certainty"). Interpreting § 101 to require "specificity" conflates the two distinct parts of the Patent Act and renders § 112(b)'s definiteness requirement redundant.

Section 101 should not be read to duplicate § 112(b). "The § 101 patent-eligibility inquiry is only a threshold test." *See Bilski,* 561 U.S. at 602. Even if an invention falls within one of the categories of eligible subject matter, the invention is also "subject to the conditions and requirements of [Title 35]." *See* 35 U.S.C. § 101; *Mayo,* 566 U.S. at 89 (quoting H.R. Rep. No. 1923, 82d Cong., 2d Sess., 6 (1952) ("A person may have 'invented' a machine or a manufacture, which may include anything under the sun that is made by man, but it is not necessarily patentable under section 101 unless the conditions of the title are fulfilled.")). The Patent Act contains three distinct patentability requirements. "Those requirements include that the invention be novel, *see* § 102, nonobvious, *see* § 103, and fully and particularly described, *see* § 112." *Bilski,* 561 U.S. at

---

Inc. v. Bandai Namco Games Am., Inc., 837 F.3d 1299, 1314 (Fed. Cir. 2016).

602. Indeed, in *Diamond v. Diehr,* the Court expressly distinguished § 101 eligibility from the conditions for patentability that follow it:

> Section 101, however, is a general statement of the type of subject matter that is eligible for patent protection "subject to the conditions and requirements of this title." Specific conditions for patentability follow . . .

Diehr, 450 U.S. at 189.

In *Mayo* 566 U.S. 66, this Court warned against conflating § 101 with other sections of the Patent Act. To be sure, *Mayo* recognized that, "in evaluating the significance of additional steps, the § 101 patent-eligibility inquiry and, say, the § 102 novelty inquiry might sometimes overlap." *Id*. at 90. But *Mayo* warned that "shift[ing] the patent-eligibility inquiry entirely to these later sections risks creating significantly greater legal uncertainty, while assuming that those sections can do work that they are not equipped to do." *Id*. at 90.

Multiple members of the Federal Circuit have, therefore, expressed concern that its jurisprudence has strayed from this guidance and begun to duplicate the patentability requirements contained in the later sections of the Patent Act. Judge Newman has proposed:

> returning to the letter of Section 101, where eligibility is recognized for 'any new and useful process, machine, manufacture, or composition of matter.' It follows that if any of these classes is claimed so broadly or vaguely or improperly as to be deemed an 'abstract idea,'

> this could be resolved on application of the requirements and conditions of patentability.

BASCOM Global Internet Servs. v. AT&T Mobility LLC,, 827 F.3d 1341, 1353 (Fed. Cir. 2016) (Newman, J., concurring in the result); *see also id.* at 1354 ("Claims that are imprecise or that read on prior art or that are unsupported by description or that are not enabled raise questions of patentability, not eligibility."). Judge Lourie similarly opined that § 101 should not be applied to do that for which § 112 is better equipped. *Ariosa Diagnostics, Inc. v. Sequenom, Inc.,* 809 F.3d 1282, 1286 (Fed. Cir. 2015) (Lourie, J., concurring in the denial of rehearing en banc) ("[T]he finer filter of § 112 might be better suited to treating these as questions of patentability, rather than reviewing them under the less-defined eligibility rules."). And now-Chief Judge Moore has criticized the Federal Circuit's use of a "blended 101/112 analysis." *American Axle & Mfg., Inc. v. Neapco Holdings LLC*, 967 F.3d 1285, 1305 (Fed. Cir. 2020*)* (Moore, J., dissenting).

Moreover, a "specificity" requirement is itself unspecific and amorphous. This Court has cautioned against adopting tests in patent cases that would "foster the innovation-discouraging 'zone of uncertainty.'" *Nautilus*, 572 U.S. at 911 (quoting *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228, 236 (1942)). The Federal Circuit's decisions articulate no standard, much less an objective standard, for assessing whether a claim is sufficiently "specific" to satisfy step one, rendering it little more than a subjective, unpredictable, and unworkable "I know it when I see it" test.

Finally, even if a "specificity" requirement at step one were well-founded as a general matter (and it is not), the Federal Circuit went beyond even its own prior cases by imposing a specially heightened "specificity" requirement for inventions related to "authentication technology." That reasoning conflicts with this Court's rejection of arguments that eligibility should be determined differently depending on the patent's technological field. *See Bilski*, 561 U.S. at 606-09 (rejecting argument that "business methods" are categorically ineligible for patenting). Nothing in the Patent Act suggests that the stringency of § 101 differs depending on the invention's technological field.

2. The Federal Circuit's "Unexpected Results" Test Is Contrary To *Alice* And *Diehr*

This case also warrants certiorari because the Federal Circuit held that three of the patents failed *Alice* step one in part because they allegedly did not achieve "unexpected results," a requirement nowhere found in *Alice* or § 101. Specifically, the court held the claims failed step one because: (1) the '539 patent "uses a combination of conventional components in a conventional way to achieve an expected result," App. 12a; (2) the '813 patent's "claimed 'encrypted authentication data' . . . achieves only expected results," App. 18a; and (3) "[w]ithout some unexpected result or improvement, the ['137 patent's] claimed idea of using three or more conventional authentication techniques to achieve a higher degree of security is abstract," App. 28a.

The Federal Circuit's "unexpected results" ruling is contrary to this Court's cases. *Alice* did not hold

that "unexpected results" are relevant at either step. *See* 573 U.S. 208. *Alice* step one is an inquiry into whether the claim is directed to an abstract idea, not into whether the benefits of the idea are unexpected. Whether the idea to which the claim is directed produces "unexpected results" has no logical bearing on whether it is concrete or abstract.

The Federal Circuit's "unexpected results" test is also contrary to *Diamond v. Diehr*, 450 U.S. 175. In *Diehr*, this Court held eligible a patent claim for using a computer and a mathematical equation to constantly measure the temperature inside a rubber mold to determine when to open the mold, thereby preventing overcuring or undercuring the rubber inside. *Id.* at 177-79. This was in contrast to the prior art industry practice of simply "calculat[ing] the cure time as the shortest time in which all parts of the product will definitely be cured," which sometimes led to over- or undercuring. *Id.* at 178. It was not "unexpected" that constantly measuring the temperature of the mold would lead to more accurate cure times. To the contrary, more accurate cure times is a completely expected result of more constant temperature measurement. If "unexpected results" were required, this Court would not have found the patent in *Diehr* to be eligible.

Again, the Federal Circuit conflated the analysis under *Alice* step one with the analysis under a different section of the patent statute. This Court has held that evidence that an invention produced unexpected results can weigh in favor of a finding that the patent claim is not obvious under § 103. *See KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 416 (2007) ("The fact that the elements worked together

in an unexpected and fruitful manner supported the conclusion that Adams' design was not obvious to those skilled in the art."). Obviousness is not, however, the inquiry required by *Alice* step one, and § 101 should not be read to duplicate § 103. *See Diehr*, 450 U.S. at 188-89 ("The 'novelty' of any element or steps in a process, or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter.").

3. The Federal Circuit's "Unconventionality" Test Is Contrary To *Alice*

Certiorari is also warranted because the Federal Circuit imposed an "unconventionality" requirement at *Alice* step one. Specifically, the court held that the patents failed step one because: (1) the '539 patent "uses a combination of conventional components in a conventional way," App. 12a; (2) the '813 patent uses "conventional tools" and "conventional data combined in a conventional way," *id.* at 17a-18a; (3) the '826 patent's authentication information and biometric information are "conventional," App. 23a; and (4) in the '137 patent, "each authentication technique is conventional," App. 27a.

This conflicts with *Alice*. *Alice* did not hold that "unconventionality" is required to survive or even relevant to *Alice* step one. *Alice*, 573 U.S. at 218-21; *see Yu v. Apple Inc.*, 1 F.4th 1040, 1049 (Fed. Cir. 2021) (Newman, J., dissenting) ("The case before us enlarges this instability in all fields, for the court holds that the question of whether the components of a new device are well-known and conventional affects § 101 eligibility, without reaching the

patentability criteria of novelty and nonobviousness."). Indeed, *Alice* demonstrates that "conventionality" is *not* determinative of step one. In *Alice*, this Court held the claims failed step *two* due to their conventional claim elements. 573 U.S. at 225. This Court did not rely on "conventionality" in its step-one ruling. *Id.* at 218-21.[2]

The decision below is also in conflict with the Federal Circuit's own precedent, reflecting an intracircuit split. In *iLife Technologies, Inc. v. Nintendo America, Inc.*, 839 F. App'x 534 (Fed. Cir. 2021), the court correctly held: "The conventionality of the claim elements is only considered at step two if the claims are deemed at step 1 to be directed to a patent ineligible concept, such as an abstract idea. A claim is not directed to an abstract idea simply because it uses conventional technology" (citation omitted). Similarly, in *Illumina, Inc. v. Ariosa Diagnostics, Inc.*, 967 F.3d 1319, 1329 (Fed. Cir. 2020), the Federal Circuit stated that, "while such

---

[2] The Federal Circuit has created similar confusion in, for example, *Yu*, 1 F.4th at 1043-44, where it held that a patent claim failed *Alice* step one in part because it relied on "well-known and conventional" components and the specification described the invention as providing "many obvious benefits and advantages." *See id.* at 1047 (Newman, J., dissenting) ("In contravention of this explicit distinction between Section 101 and Section 102, the majority now holds that the '289 camera is an abstract idea because the camera's components were well-known and conventional and perform only their basic functions. That is not the realm of Section 101 eligibility."). *See also Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1346 (Fed. Cir. 2018) (holding that patent claims were directed to an abstract idea at step one because "they consist of generic and conventional information acquisition and organization steps").

conventionality considerations may be relevant to the inquiry under *Alice*/*Mayo* step two . . . they do not impact the *Alice*/*Mayo* step one question whether the claims themselves are directed to a natural phenomenon." The role of "conventionality" at *Alice* step one in the Federal Circuit, therefore, appears to turn on the constitution of the panel, rather than this Court's precedent.

Nor does requiring unconventionality at step one make sense. Whether the idea to which a claim is directed is concrete or abstract has nothing to do with the conventionality of the claim limitations. For example, the elements that comprise an ordinary hammer, such as a handle and an attached head, are conventional, but a physical hammer is not an abstract idea.

4. The Federal Circuit's Application Of *Alice* Step One Eviscerates Step Two

The Federal Circuit created further conflict with *Alice* by applying step one so as to effectively eliminate the need for step two. Under *Alice,* if a court determines that a claim is "directed to" an abstract idea, the court must then determine whether the claim, nevertheless, "contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application. 566 U.S. at 71, 79) (internal quotation marks omitted). Here, the Federal Circuit's application of step one predetermined the outcome without regard for step two. By effectively collapsing *Alice*'s two steps into one, the opinion further conflicts with *Alice* and warrants certiorari.

As described *supra*, the Federal Circuit held that the patent claims fail *Alice* step one due to their alleged lack of "specificity," "unexpected results," and "unconventional" limitations. The court then applied substantially the same analysis to conclude the claims lack an inventive concept and therefore fail *Alice* step two. Specifically, the Federal Circuit held that the claims failed step two because: (1) the '539 patent's method is "conventional and long-standing," App. 13a; (2) the '813 patent was "merely a combination of known authentication techniques that yields only expected results" and "conventional authentication techniques" that failed to "achieve[] more than the expected sum of the security provided by each technique," App. 18a-19a; (3) the '826 patent claimed "conventional ways to perform authentication" and "combined non-specific, conventional authentication techniques," App. 23a-4a; and (4) the '137 patent claimed "devices and functions" that are "conventional" and used "conventional location for the authentication functionality," "yield[ed] expected additory amounts of security," and provided no "unexpected improvement beyond the expected sum of the security benefits of each individual technique," App 29a. The Federal Circuit even explained its step-two holdings by cross-referencing its step-one analysis. App. 18a-19a (prefacing its '813 patent step-two analysis with "As we explained above [with respect to step one]" and concluding with "as we have previously explained [in connection with step one]"); App. 29a (similar with respect to the '137 patent).

This confirms that requiring "unconventionality," "specificity," or "expected results" to pass step one is contrary to *Alice*. The decision conflicts with *Alice*

because it effectively renders *Alice*'s two steps duplicative of one another. Any claim that fails step one due to "conventionality," "expected results," or lack of "specificity" will also fail step two if that same analysis is reapplied.[3] The opinion below, therefore, effectively truncates the two-step analysis dictated by *Alice.*

B. This Case Presents Exceptionally Important Issues Of Patent Law

Predictable patent eligibility rulings are critical to the health of the patent system and the economy. This case thus presents an exceptionally important issue of patent law, providing further reason for review. Former USPTO directors, the Solicitor General, congressmen, commentators, and current and former judges on the Federal Circuit have all bemoaned the current state of § 101 case law and the seemingly arbitrary and inconsistent outcomes it has produced.

In response to post-*Alice* CVSG invitations, the Solicitor General has opined that "this Court's recent decisions have fostered uncertainty concerning those

---

[3] The Federal Circuit repeated this same flawed analysis in *Yu*, 1 F.4th 1040, where it first held that the patent claims failed *Alice* step one due to their use of "conventional components," *id.* at 1043, and then held that they also failed step two due to those same conventional components, *id*. at 1045. Similarly, in *Interval Licensing*, 896 F.3d 1335, the Federal Circuit first held that the patent claims failed step one because they were directed to abstract ideas because they recited conventional steps, *id.* at 1345-46, and then held that the claims also failed step two for the same reason, *id*. at 1347-48.

substantive Section 101 standards," that "[t]he Court should grant review in an appropriate case to clarify the substantive Section 101 standards," Brief for the United States, *HP Inc. v. Berkheimer,* No. 18-415, at 10, and that "[t]he confusion created by this Court's recent Section 101 precedents warrants review in an appropriate case," Brief for the United States, *Hikma Pharms. USA Inc. v. Vanda Pharms. Inc.,* No. 18-817, at 8.

The calls for guidance from the judges of the Federal Circuit are overwhelming. The Federal Circuit is "at a loss as to how to uniformly apply § 101" and its active judges have "unanimous[ly]" made an "unprecedented plea for guidance" from this Court. *American Axle,* 977 F.3d at 1382 (Moore, J., concurring). According to Judge Moore, the doctrine has devolved into an inconsistent, "panel-dependent body of law." *Id. See also Interval Licensing*, 896 F.3d at 1348 (Plager, J., concurring in part and dissenting in part) ("The law, as I shall explain, renders it near impossible to know with any certainty whether the invention is or is not patent eligible."). As Judge Plager has noted, the *Alice* step one jurisprudence is a "definitional morass" that lacks a "single, succinct, usable definition anywhere" for what constitutes an abstract idea. *Id.* at 1350. The result is "little consensus among trial judges (or appellate judges for that matter) regarding whether a particular case will prove to have a patent with claims directed to an abstract idea." *Id.* at 1354-55. *See also Smart Sys. Innovations, LLC v. Chi. Transit Auth.,* 873 F.3d 1364, 1377 (Fed. Cir. 2017) (Linn, J. concurring in part and dissenting in part) ("[T]he abstract idea exception is almost impossible to apply consistently and coherently . . . . The problem with

this test . . . is that it is indeterminate and often leads to arbitrary results.").

The unpredictable application of *Alice* has far-reaching consequences. The Federal Circuit's "rulings on patent eligibility have become so diverse and unpredictable as to have a serious effect on the innovation incentive in all fields of technology. . . . [T]he victims are the national interest in an innovative industrial economy, and the public interest in the fruits of technological advance." *American Axle & Manufacturing, Inc. v. Neapco Holdings LLC,* 966 F.3d 1347, 1357 (Fed. Cir. 2020) (Newman, J., dissenting from denial of rehearing en banc). This unpredictability is "destroying the ability of American businesses to invest with predictability." *American Axle,* 977 F.3d at 1382 (Moore, J., concurring).

Former USPTO directors have echoed the Federal Circuit's pleas for guidance. Former director Andrei Iancu recently described the state of § 101 law as an "issue that has plagued our system for the past decade." Remarks by Director Iancu (Jan. 19, 2021).[4] He emphasized, "We must resolve this issue, and we must resolve it now. If not, we risk our nation being left behind as others fortify their IP laws and race towards technological dominance in the Fourth Industrial Revolution." *Id.* Former USPTO director David Kappos agreed:

---

[4] *Available at* https://www.uspto.gov/about-us/news-updates/remarks-director-iancu-us-chamber-commerce-event-how-innovation-and#.

> Our current patent eligibility law truly is a mess. The Supreme Court, Federal Circuit, district courts, and USPTO are all spinning their wheels on decisions that are irreconcilable, incoherent, and against our national interest. . . . [U]nder current U.S. law governing patent eligibility, it is easier to secure patent protection for critical life sciences and information technology inventions in the People's Republic of China and in Europe, than in the U.S.

David J. Kappos, Oral Testimony Before the U.S. Senate Sub-Committee on Intellectual Property (June 4, 2019).[5]

Members of Congress have similarly expressed concern about the damage that the unpredictability of patent eligibility has had on the Nation's innovation and economic progress. According to Senator Tillis:

> The current state of patent eligibility is undermining research, development, and innovation across many industries . . . . [T]he lack of predictability and certainty under the current law will prevent the innovation ecosystem from fully realizing its potential. . . . This uncertainty has caused many innovators to simply abandon future attempts at research and development or innovation. Why would anyone in their right mind risk millions if not billions of dollars to develop a product when

---

[5] *Available at* https://www.judiciary.senate.gov/imo/media/doc/Kappos%20Testimony.pdf

> they have no idea if they're eligible for protection? From a business perspective, it simply isn't worth the risk for many endeavors.

The State of Patent Eligibility in America, Part I, 116th Cong. 3 (June 4, 2019) (statement of Sen. Tillis).[6] Senator Coons echoed these concerns:

> Recent decisions of the Supreme Court over a decade have clouded the waters regarding exactly what types of inventions merit protection . . . . Determining whether an invention is an abstract idea, for example, has proven to be a truly unpredictable test for eligibility with many now viewing the results as turning on the luck of the draw depending on which examiner or judge reviews them.

The State of Patent Eligibility in America, Part I, 116th Cong. 3 (June 4, 2019) (statement of Sen. Tillis).[7]

Retired Federal Circuit Chief Judge Michel has also expressed the view that reform of the patent eligibility case law is urgently required:

> In my view, recent cases are unclear, inconsistent with one another and confusing. I myself cannot reconcile the cases. That applies equally to Supreme Court and Federal Circuit cases. Nor can I predict outcomes in

---

[6] *Available at* https://www.judiciary.senate.gov/meetings/the-state-of-patent-eligibility-in-america-part-i.

[7] *Available at* https://www.judiciary.senate.gov/meetings/the-state-of-patent-eligibility-in-america-part-i.

> individual cases with any confidence since the law keeps changing year after year. If I, as a judge with 22 years of experience deciding patent cases on the Federal Circuit's bench, cannot predict outcomes based on case law, how can we expect patent examiners, trial judges, inventors and investors to do so?

Testimony of Hon. Paul R. Michel Before the Subcommittee on Intellectual Property of the S. Comm. on the Judiciary, 116th Cong. 2 (June 4, 2019);[8] *see also* Supplemental Statement of Judge Paul R. Michel (Ret.) to the United States House of Representatives Committee on the Judiciary, September 12, 2017 ("P]atent eligibility law under § 101 has descended into chaos . . . that is devastating American business, including high tech, manufacturing, biotech, and pharmaceutical industries.").[9]

The National Security Commission on Artificial Intelligence found that "[t]he legal uncertainty for U.S. innovators and companies as to whether their inventions will be eligible for patent protection or susceptible to invalidation once granted is pervasive. This uncertainty in turn has impacted investments in AI and technologies critical to national security."

---

[8] *Available at* https://www.judiciary.senate.gov/imo/media/doc/Michel%20Testimony.pdf.

[9] *Available at* https://innovationalliance.net/wp-content/uploads/2017/09/Supplemental-Statement-of-Paul-R-Michel-Sept-12-2017.pdf

National Security Commission on Artificial Intelligence, Final Report 469 (2021).[10]

Likewise, the USPTO issued guidance to patent examiners lamenting the inconsistency and confusion in the Federal Circuit's "abstract idea" case law:

> In addition, similar subject matter has been described [by the Federal Circuit] both as abstract and not abstract in different cases. The growing body of precedent has become increasingly more difficult for examiners to apply in a predictable manner, and concerns have been raised that different examiners within and between technology centers may reach inconsistent results.

2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50, 52 (Jan. 7, 2019).

C. This Case Is An Ideal Vehicle To Clarify *Alice* Step One

This is an opportune case for this Court to clarify the appropriate standard under *Alice* step one to determine whether a patent claim is directed to ineligible subject matter, such as an abstract idea, and if so, how to determine what that abstract idea is.

First, USR's patents involve computers, software, electronic signal processing, and communication networks. According to a recent study of patent

---

[10] *Available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

eligibility decisions between 2014-2019, "90 percent of post-*Alice* decisions are in the software/IT industry." Mark A. Lemley & Samantha Zyontz, *Does Alice Target Patent Trolls?,* 18 J. Empirical Legal Stud. 47, 67 (2021). This Court should, therefore, clarify its abstract idea jurisprudence in a case, such as this, involving software or information technology so that its ruling may provide guidance for the largest number of pending and future disputes.

Second, this case is an ideal vehicle because USR's patents have survived multiple post-issue challenges to their validity in the Patent Office. The Patent Trial and Appeal Board rejected Apple's and Visa's petitions for *inter partes* and covered business method review, issuing multiple decisions upholding the patents' validity against obviousness and novelty challenges under § 102 and § 103. This case is, therefore, not complicated by extraneous invalidity issues. Nor is the impact of this Court's decision likely to be obviated by a subsequent invalidation of USR's patents on other grounds.

Third, the Federal Circuit's decision is published and precedential. It therefore represents the court's careful and deliberate consideration and full reasoning and will guide the court's future application of *Alice* step one.

Fourth, four different decision makers have applied *Alice* step one to USR's patents and arrived at four different conclusions. The PTAB found, at *Alice* step one, that the '813 patent was not directed to an abstract idea, but instead to the concrete idea of:

> an improvement in the security of mobile devices by using a biometric sensor, a user interface, a communication interface, and a processor working together to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be used fraudulently in subsequent transactions.

C.A. Appx5266. The magistrate judge agreed, concluding that USR's patents were not directed to abstract ideas at *Alice* step one, but instead represented technological improvements to computer functionality.

The district court and the Federal Circuit, however, disagreed and held that the claims were directed to abstract ideas. Those courts could not agree, however, on what those abstract ideas were, as the below table illustrates.

No.	District Court's Abstract Idea	Federal Circuit's Abstract Idea
'539	"obtaining the secure verification of a user's identity to enable a transaction"	"verifying the identity of a user to facilitate an economic transaction"
'813	"a device [that] collects and examines data to authenticate the user's identity"	"an electronic ID device that includes a biometric sensor, user interface, communication interface, and processor working together to (1) authenticate the user

No.	District Court's Abstract Idea	Federal Circuit's Abstract Idea
		based on two factors—biometric information and secret information known to the user—and (2) generate encrypted authentication information to send to the secure registry through a point-of-sale device" or "collecting and examining data to enable authentication"
'826	"secured verification of a person's identity"	"multi-factor authentication of a user's identity using two devices to enable a transaction"
'137	"a system for authenticating a user for enabling a transaction"	"multi-factor authentication of a user's identity using two devices to enable a transaction"

The Federal Circuit provided no explanation for its disagreement with the district court's formulation of the patents' alleged abstract ideas, demonstrating

the arbitrariness of its *Alice* step-one jurisprudence.[11]

That four sets of decision makers not only cannot agree on whether the patents are directed to abstract ideas under *Alice* step one, but also cannot agree on what those abstract ideas are not only illustrates the need for this Court's clarification of that standard, but also the value of granting certiorari in this specific case. This Court's analysis will be aided by these several attempts to apply *Alice* to these specific patents.[12]

---

[11] The Federal Circuit has, in other cases, declined to even articulate at step one what the patent claim is directed to. *See Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1307 (Fed. Cir. 2016) (Reyna, J., dissenting) ("The majority avoids determining whether the asserted claims are directed to an abstract idea, or even identifying what the underlying abstract idea is.").

[12] This case also illustrates the arbitrariness of the Federal Circuit's *Alice* decisions. Shortly after it issued its decision in this case invalidating USR's patents, the Federal Circuit reached the opposite conclusion with respect to a very similar patent claiming "a method of authenticating the identity of a user performing a transaction at a terminal (e.g., a computer), including activating an authentication function on the user's mobile device." *CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC*, 15 F.4th 1091, 1092 (Fed. Cir. 2021). In *CosmoKey,* the court skipped *Alice* step one entirely and held the claim patentable at step two, a holding that former Judge Michel characterized as "on its face . . . difficult to reconcile with the opposite outcome in the present case." Brief of Amicus Curiae Paul R. Michel In Support of Appellant's Combined Petition For Rehearing and Rehearing En Banc, *Universal Secure Registry LLC v. Apple Inc.*, No. 20-2044, Dkt. 65 (Fed. Cir.).

II. In The Alternative, The Court Should Hold This Petition Pending Resolution Of *American Axle & Manufacturing, Inc. v. Neapco Holdings LLC, et al.*, No. 20-891

The question presented is similar to the question presented in in the pending petition for certiorari in *American Axle & Manufacturing, Inc. v. Neapco Holdings LLC,* et al., No. 20-891 (filed December 28, 2020), and the Court has asked for the views of the Solicitor General on whether certiorari should be granted in that case. If the Court does not grant this petition, it should at a minimum hold the petition pending resolution of the *American Axle* petition. If the Court the grants certiorari in *American Axle*, it should grant certiorari here, vacate the decision below, and remand for further consideration in light of its *American Axle* opinion.

CONCLUSION

The petition should be granted or, in the alternative, held pending resolution of *American Axle & Manufacturing, Inc. v. Neapco Holdings LLC, et al.*, No. 20-891.

Respectfully submitted,

KATHLEEN M. SULLIVAN
Counsel of Record
TIGRAN GULEDJIAN
CHRISTOPHER MATHEWS
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
865 S. Figueroa St. 10th Floor
Los Angeles, CA 90017
(213) 443-3000
kathleensullivan@
quinnemanuel.com

KEVIN A. SMITH
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
50 California St. 22nd Floor
San Francisco, CA 94111

Counsel for Petitioner

January 27, 2022

APPENDIX

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2020-2044

UNIVERSAL SECURE REGISTRY LLC,

Plaintiff-Appellant

v.

APPLE INC., VISA INC., VISA U.S.A. INC.,

Defendants-Appellees

Appeal from the United States District Court for the District of Delaware in No. 1:17-cv-00585-CFC-SRF, Judge Colm F. Connolly.

Decided: August 26, 2021

KATHLEEN M. SULLIVAN, Quinn Emanuel Urquhart & Sullivan, LLP, New York, NY, argued for plaintiff-appellant. Also represented by BRIAN MACK, KEVIN ALEXANDER SMITH, San Francisco, CA; TIGRAN GULEDJIAN, CHRISTOPHER MATHEWS, Los Angeles, CA.

MARK D. SELWYN, Wilmer Cutler Pickering Hale and Dorr LLP, Palo Alto, CA, argued for defendant-appellee Apple Inc. Also represented by LIV LEILA HERRIOT, THOMAS GREGORY SPRANKLING; MONICA GREWAL, Boston, MA.

STEFFEN NATHANAEL JOHNSON, Wilson, Sonsini, Goodrich & Rosati, PC, Washington, DC, argued for defendants-appellees Visa Inc., Visa U.S.A. Inc. Also represented by MATTHEW A. ARGENTI, JAMES C. YOON, Palo Alto, CA.

Before TARANTO, WALLACH,* and STOLL, *Circuit Judges*.

STOLL, *Circuit Judge*.

Universal Secure Registry LLC (USR) appeals the United States District Court for the District of Delaware's dismissal of certain patent infringement allegations against Apple Inc., Visa Inc., and Visa U.S.A. Inc. (collectively, "Apple") under Rule 12(b)(6) of the Federal Rules of Civil Procedure. The district court held all claims of four asserted patents owned by USR ineligible under 35 U.S.C. § 101. Because we conclude that all claims of the asserted patents are directed to an abstract idea and that the claims contain no additional elements that transform them into a patent-eligible application of the abstract idea, we affirm.

BACKGROUND

I

USR sued Apple for allegedly infringing all claims of U.S. Patent Nos. 8,856,539; 8,577,813; 9,100,826; and 9,530,137 (collectively, the "asserted patents"). The '137 patent is a continuation of the '826 patent. Although the patents are otherwise unrelated, they are directed to similar technology—securing electronic

---

* Circuit Judge Evan J. Wallach assumed senior status on May 31, 2021.

payment transactions. As USR explained in its opening brief, its patents "address the need for technology that allows consumers to conveniently make payment-card [e.g., credit card] transactions without a magnetic-stripe reader and with a high degree of security." Appellant's Br. 7. "For example, it allows a person to purchase goods without providing credit card information to the merchant, thereby preventing the credit card information from being stolen or used fraudulently." *Id.* at 9.

II

Apple moved to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6), arguing that the asserted patents claimed patent-ineligible subject matter under 35 U.S.C. § 101. The magistrate judge determined that all the representative claims are directed to a non-abstract idea. *Universal Secure Registry, LLC v. Apple Inc.*, No. 17-cv-00585, 2018 WL 4502062, at *8–11 (D. Del. Sept. 19, 2018). The magistrate judge explained that the '539 patent claims are "not directed to an abstract idea because 'the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity.'" *Id.* at *8 (quoting *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017)). Of particular importance to the magistrate judge was the conclusion that the claimed invention provided a more secure authentication system. *See id.* at *9.

The district court disagreed, concluding that the representative claims fail at both steps one and two of *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). *Universal Secure Registry LLC* (*USR*) *v. Apple Inc.*, 469 F. Supp. 3d 231, 236–37 (D. Del. 2020). The

district court explained that the claimed invention was directed to the abstract idea of "the secure verification of a person's identity" and that the patents do not disclose an inventive concept—including an improvement in computer functionality—that transforms the abstract idea into a patent-eligible application. *Id.* Accordingly, the district court granted Apple's motion to dismiss for failure to state a claim under Rule 12(b)(6). *Id.* at 240.

USR appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

We apply regional circuit law when reviewing a district court's dismissal for failure to state a claim under Rule 12(b)(6). *XY, LLC v. Trans Ova Genetics, LC*, 968 F.3d 1323, 1329 (Fed. Cir. 2020). The Third Circuit reviews such dismissals de novo, accepting as true all factual allegations in the complaint and viewing those facts in the light most favorable to the non-moving party. *Klotz v. Celentano Stadtmauer & Walentowicz LLP*, 991 F.3d 458, 462 (3d Cir. 2021) (citing *Foglia v. Renal Ventures Mgmt., LLC*, 754 F.3d 153, 154 n.1 (3d Cir. 2014)).

Patent eligibility under § 101 is a question of law based on underlying facts, so we review a district court's ultimate conclusion on patent eligibility de novo. *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1342 (Fed. Cir. 2018). We have held that patent eligibility can be determined at the Rule 12(b)(6) stage "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018).

I

Section 101 defines patent-eligible subject matter as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. Long-standing judicial exceptions, however, provide that laws of nature, natural phenomena, and abstract ideas are not eligible for patenting. *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 765 (Fed. Cir. 2019) (citing *Alice*, 573 U.S. at 216).

The Supreme Court has articulated a two-step test for examining patent eligibility when a patent claim is alleged to involve one of these three types of subject matter. *See Alice*, 573 U.S. at 217–18. The first step of the *Alice* test requires a court to determine whether the claims at issue are directed to a patent-ineligible concept, such as an abstract idea. *Id.* at 218. "[T]he claims are considered in their entirety to ascertain whether their character as a whole is directed to excluded subject matter." *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016) (quoting *Internet Pats. Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)). If the claims are directed to a patent-ineligible concept, the second step of the *Alice* test requires a court to "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 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72, 78–79 (2012)). This inventive concept must do more than simply recite "well-understood, routine, conventional activity." *Mayo*, 566 U.S. at 79–80.

In cases involving authentication technology, patent eligibility often turns on whether the claims provide

sufficient specificity to constitute an improvement to computer functionality itself. For example, in *Secured Mail Solutions LLC v. Universal Wilde, Inc.*, we held that claims directed to using a marking (e.g., a conventional barcode) affixed to the outside of a mail object to communicate information about the mail object, including claims reciting a method for verifying the authenticity of the mail object, were abstract. 873 F.3d 905, 907, 910–11 (Fed. Cir. 2017). We explained that the claims were not directed to specific details of the barcode or of the equipment for generating and processing the barcode. *See id.* at 910. Nor was there a description of how the barcode was generated, or how that barcode was different from long-standing identification practices. *See id.* At step two, we determined that there was no inventive concept that transformed the claimed abstract idea into a patent-eligible application of the abstract idea. *See id.* at 912. We explained that the claims recited well-known and conventional ways to verify an object using a barcode and to allow generic communication between a sender and recipient using generic computer technology, and that the patents themselves suggested that all the hardware used was conventional. *See id.*

In *Electronic Communication Technologies, LLC v. ShoppersChoice.com, LLC*, we drew a similar conclusion about claims focused on monitoring the location of a "mobile thing" and using authentication software to increase security. 958 F.3d 1178, 1181 (Fed. Cir. 2020). As to the authentication limitations—"namely, enabling a first party to input authentication information, storing the authentication information, and providing the authentication information along with the advance notice of arrival to help ensure the customer that the notice was initiated by an author-

ized source"—we determined that these limitations were themselves abstract and thus were not an inventive concept. *Id.* We pointed to the specification, which stated that the claimed "authentication information" could be essentially any information recognizable to the party being contacted. *Id.* We also noted that businesses have long been recording customer information that would qualify as authentication information as broadly defined in the specification. *See id.* at 1182.

Similarly, in *Solutran, Inc. v. Elavon, Inc.*, we held ineligible claims that recited a method for electronically processing checks, which included electronically verifying the accuracy of a transaction to avoid check fraud, because the claims were directed to a long-standing commercial practice of crediting a merchant's account as soon as possible. 931 F.3d 1161, 1163, 1167 (Fed. Cir. 2019). We recognized that the claims only recited conventional steps that were not directed to an improvement to the way computers operate, noting that the patent specification explained that "verifying the accuracy of the transaction information . . . was already common." *Id.* at 1167. At step two, we rejected the argument that reordering these conventional steps constituted an inventive concept, and held that using a general-purpose computer and scanner to perform the conventional activities of transaction verification does not amount to an inventive concept. *Id.* at 1168–69.

Finally, in *Prism Technologies LLC v. T-Mobile USA, Inc.*, the claims broadly recited "receiving" identity data of a client computer, "authenticating" the identity of the data, "authorizing" the client computer, and "permitting access" to the client computer. 696 F. App'x 1014, 1016 (Fed. Cir. 2017). We held that the

claims at issue were directed to the abstract idea of "providing restricted access to resources" because the claims did not cover a "concrete, specific solution." *Id.* at 1017. Rather, the claims merely recited generic steps typical of any conventional process for restricting access, including processes that predated computers. *Id.* At step two, we determined that the asserted claims recited conventional generic computer components employed in a customary manner such that they were insufficient to transform the abstract idea into a patent-eligible invention. *Id.*

II

With this precedent in mind, we turn to the patent claims at issue in this case. We address each patent in turn.

A

We first consider the claims of the '539 patent. The '539 patent is titled "Universal Secure Registry" and explains that most people carry multiple forms of identification to verify their identities and make purchases, '539 patent col. 1 ll. 53–67, but that they may not always want to disclose their personal information during financial transactions, *id.* at col. 2 ll. 1–27. Thus, the '539 patent proposes "an identification system that will enable a person to be identified or verified . . . and/or authenticated without necessitating the provision of any personal information." *Id.* at col. 2 l. 64–col. 3 l. 1. The patent purports to accomplish this goal through use of a Universal Secure Registry or "USR system or database . . . [that] may take the place of multiple conventional forms of identification." *Id.* at col. 3 ll. 22–24. Access to the USR system may be gained through a user's electronic ID device, which may be a smart card,

cell phone, pager, wristwatch, computer, personal digital assistant, key fob, or other commonly available electronic devices. *Id.* at col. 3 l. 64–col. 4 l. 4.

One embodiment of the invention facilitates purchasing goods or services without revealing personal financial information to a merchant. *See id.* at col. 11 l. 46–col. 12 l. 18. When a user initiates a purchase, the user enters a secret code in the user's electronic ID device to cause the ID device to generate a one-time code. *Id.* at col. 11 ll. 51–56. After the user presents the one-time code to the merchant, the merchant transmits the code, the store number, the amount of the purchase, and the time of receipt to the credit card company. *Id.* at col. 11 ll. 56–59. The credit card company then passes the code to the USR system, which determines if the code is valid and, "if valid, accesses the user's credit card information and transmits the appropriate credit card number to the credit card company." *Id.* at col. 11 ll. 59–65. The credit card company then checks the credit worthiness of the user and either "declines the card or debits the user's account in accordance with its standard transaction processing system." *Id.* at col. 12 ll. 6–9. "The credit card company then notifies the merchant of the result of the transaction." *Id.* at col. 12 ll. 9–11.

> Claim 22 is representative of the '539 patent claims at issue and states as follows:
>
> 22. A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

> receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;
>
> mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;
>
> determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;
>
> accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;
>
> providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction; and
>
> enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information.

Id. at col. 20 ll. 4–31.

The district court held that claim 22 is not materially different from the claims at issue in *Prism*. As discussed above, in *Prism*, we determined that the claims were directed to the process of "(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the

identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources." *Prism*, 696 F. App'x at 1017. Here, the district court stated that claim 22 requires the following steps:

> (1) "receiving" a transaction request with a time-varying multicharacter code and "an indication of" the merchant requesting the transaction; (2) "mapping" the time-varying multicharacter code to the identity of the customer in question; (3) "determining" whether the merchant's access to the customer's secure data complies with any restrictions; (4) "accessing" the customer's account information; (5) "providing" the account identifying information to a third party without providing that information to the merchant; and (6) "enabling or denying" the merchant to perform the transaction without obtaining knowledge of the customer's identifying information.

USR, 469 F. Supp. 3d at 237. Based on the similarities between these steps and those in the claims at issue in *Prism*, the district court determined that claim 22 is directed to "the abstract idea of obtaining the secure verification of a user's identity to enable a transaction." *Id.*

While we see differences between claim 22 and the claims at issue in *Prism*, we agree with the district court that, like the claims at issue in *Prism*, claim 22 is directed to an abstract idea. The claims are directed to a method for enabling a transaction between a user and a merchant, where the merchant is given a time-varying code instead of the user's secure (credit card)

information. The time-varying code is used to access a database that indicates any restrictions on the user's transactions with the merchant and also allows a third party or credit card company to approve or deny the transaction based on the secure information without the provider gaining access to the secure information. In our view, the claims "simply recite conventional actions in a generic way" (e.g., receiving a transaction request, verifying the identity of a customer and merchant, allowing a transaction) and "do not purport to improve any underlying technology." *Solutran*, 931 F.3d at 1168. Accordingly, the claims are directed to an abstract idea under *Alice* step one.

USR cites *Ancora Technologies, Inc. v. HTC America, Inc.*, to assert that the claims' recitation of a time-varying multicharacter code used in combination with additional intermediaries constitutes a specific technique that departs from earlier approaches to solve a specific computer problem. 908 F.3d 1343 (Fed. Cir. 2018). We are unpersuaded. In *Ancora*, the claimed invention identified a specific technique for addressing the vulnerability of license-authorization software to hacking in an unexpected way—by storing the software license record in the computer's BIOS memory. *Id.* at 1348–49. Using the BIOS memory to assist with software verification was unexpected because it had never previously been used in that way. *Id.* The claimed invention of the '539 patent, on the other hand, uses a combination of conventional components in a conventional way to achieve an expected result. *See, e.g.*, '539 patent col. 7 ll. 30–36 (disclosing a SecurIDTM card or its equivalent as an example of a single use code generator). While we appreciate that the claims here are closer to the demarcation line between what is abstract and non-abstract than the

claims in *Prism*, we conclude that, at *Alice* step one, the asserted claims are directed to a method for verifying the identity of a user to facilitate an economic transaction, for which computers are merely used in a conventional way, rather than a technological improvement to computer functionality itself.

Turning to *Alice* step two, the district court rejected USR's argument that the claim's recitations of (1) time-varying codes and (2) sending data to a third-party as opposed to the merchant each rise to the level of an inventive concept. *USR*, 469 F. Supp. 3d at 238. We agree. Regarding USR's first argument, the patent itself acknowledges that the claimed step of generating time-varying codes for authentication of a user is conventional and long-standing. '539 patent col. 8 ll. 17–35 (disclosing use of a "SecurIDTM card available from RSA Security," which "retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code").

And with regard to USR's second argument—that the step of bypassing the merchant's computer constitutes an inventive concept—USR cites *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, where we determined that claims directed to a method and system of filtering Internet content using the individual account association capability of some Internet Service Provider (ISP) servers were a "technical improvement over prior art ways of filtering such content." 827 F.3d 1341, 1350, 1352 (Fed. Cir. 2016). In that case, we reasoned that although "[f]iltering content on the Internet was already a known concept, . . . the patent describes how its particular arrangement of elements is a technical improvement over prior art ways of filtering such

content." *Id.* at 1350. Unlike was the case in *BASCOM*, however, the Supreme Court has previously held the use of a third-party intermediary in a financial transaction to be an ineligible abstract idea. *Alice*, 573 U.S. at 219–20. In *Alice*, the claims involved "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Id.* at 219. Similarly, the claims here involve allowing a financial transaction between two parties using a third-party intermediary to mitigate information security risks. Because sending data to a third-party as opposed to the merchant is itself an abstract idea, it cannot serve as an inventive concept. *BASCOM*, 827 F.3d at 1349 ("An inventive concept that transforms the abstract idea into a patent-eligible invention must be significantly more than the abstract idea itself . . . ." (citing *Alice*, 573 U.S. at 223–24)).

B

We next consider the claims of the '813 patent. The '813 patent is also titled "Universal Secure Registry" and the invention bears resemblance to that in the '539 patent. The '813 patent discloses combined use of a user device (e.g., cell phone), a point-of-sale (POS) device, and a universal secure registry to facilitate financial transactions. '813 patent col. 43 ll. 6–15. One embodiment of the claimed invention contemplates the user device communicating with a secure database in the secure registry, which stores account information, such as credit card and debit card account information, for multiple accounts. *Id.* at col. 44 ll. 39–53. This allows users to employ a single user device or cell phone to conduct financial transactions at a POS device using a plurality of different credit or debit accounts. *Id.* at col. 45 ll. 4–17.

Before the user device can access the secure registry, however, certain authentication processes must be completed. One embodiment contemplates first restricting access to the user device until the user has been authenticated using biometric input provided to the user device. *Id.* at col. 46 ll. 37–41. Next, the secure registry also requires that the user be authenticated before account information is accessed. *Id.* at col. 45 ll. 18–20. Some embodiments employ a multi-factor authentication process whereby encrypted authentication information is generated by the user device. *Id.* at col. 46 ll. 14–36. That is, the claimed invention can authenticate the user based on a combination of two or more of (1) "something the user knows" (e.g., PIN number); (2) "something the user is" (e.g., a biometric measurement as detected by a biometric sensor); (3) "something that the user has" (e.g., cell phone serial number); and (4) an "account selected by the user for the current transaction" (e.g., the transaction for which the authentication is being completed). *Id.* at col. 45 l. 63–col. 46 l. 21. This encrypted authentication information is then communicated to the secure registry for authentication through the POS device and, if authentication is successful, the transaction and access to the user's account is permitted. *Id.* at col. 46 ll. 27–36.

Claim 1 of the '813 patent is representative:

> 1. An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> a biometric sensor configured to receive a biometric input provided by the user;

a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;

a communication interface configured to communicate with a secure registry;

a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and

wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

Id. at col. 51 l. 65–col. 52 l. 29.

The district court held that the claims are directed to the abstract idea of "collect[ing] and examin[ing] data to authenticate the user's identity." *USR*, 469 F. Supp. 3d at 239. We agree with the district court that the claims are directed to an abstract idea, not a technological solution to a technological problem, as USR asserts. In our view, the claims are directed to an electronic ID device that includes a biometric sensor, user interface, communication interface, and processor working together to (1) authenticate the user based on two factors—biometric information and secret information known to the user—and (2) generate encrypted authentication information to send to the secure registry through a point-of-sale device. There is no description in the patent of a specific technical solution by which the biometric information or the secret information is generated, or by which the authentication information is generated and transmitted. In our view, as with the '539 patent, the claims recite "conventional actions in a generic way"—e.g., authenticating a user using conventional tools and generating and transmitting that authentication—without "improv[ing] any underlying technology." *Solutran*, 931 F.3d at 1168. Accordingly, the claims are directed to an abstract idea under *Alice* step one.

USR asserts that the claims solve a problem in an existing technological process using a novel form of data the patent describes as "encrypted authentication information." Appellant's Br. 44. USR reasons that, like the claimed invention in *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), this encrypted authentication information is a non-abstract improvement in computer functionality. Appellant's Br. 45. We are not persuaded. In *Finjan*, we determined that the claimed invention was not

abstract because it claimed the use of a "behavior-based" virus scan that was able to identify and compile unique information about potentially hostile operations, while the traditional scan method was limited to recognizing the presence of previously identified viruses. 879 F.3d at 1304. Unlike in *Finjan*, the claimed "encrypted authentication data" here is merely a collection of conventional data combined in a conventional way that achieves only expected results. *See* '813 patent col. 46 ll. 21–27 ("For example, in one embodiment, encrypted authentication information is generated from a non-predictable value generated by the user device 352, identifying information for the selected user account 360, and at least one of the biometric information and secret information the user knows (for example, a PIN)."). We thus conclude that the claims are directed to the abstract idea of collecting and examining data to enable authentication.

Turning to *Alice* step two, the district court explained that the specification "describes the Electronic ID Device as 'any type of electronic device' capable of accessing a secure identification system database." *USR*, 469 F. Supp. 3d at 239 (citation omitted). The court added that the patent also "describes the device as consisting of well-known, generic components, including a computer processor." *Id.* at 239–40. Based on this, the court determined that the claims do not recite an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application.

We agree with the district court that the claims fail to recite an inventive concept that would transform the abstract idea into patentable subject matter. As we explained above, the "encrypted authentication

data" is merely a combination of known authentication techniques that yields only expected results. For example, the '813 patent specification explains that a one-time non-predictable code can be generated by the "SecurIDTM card available from RSA Security," as well as "other smart cards" or an algorithm programmed onto a processor. '813 patent col. 12 l. 45–col. 13 l. 5. The '813 patent specification also discloses that identifying information may include something as well-known as "a unique serial number" on a check. *Id.* at col. 17 ll. 26–29. Moreover, the specification explains that a user may be verified using "any combination of a memorized PIN number or code, biometric information such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device." *Id.* at col. 4 ll. 29–34; *see also id.* at col. 2 ll. 59–64 (disclosing that prior art uses "biometric sensors that sense one or more biometric feature[s]"). There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique. *Cf. TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1295–96 (Fed. Cir. 2020) (explaining that multilevel security using a combination of secure labeling with encryption constituted an inventive concept where the patent specification made clear that "the focus of the claimed advance is on improving . . . a data network used for broadcasting a file to a large audience" and the improvement was "an efficient way for the sender to permit different parts of the audience to see different parts of the file"). In other words, the combination of these long-standing conventional methods of

authentication yields expected results of an additive increase in security. Moreover, as we have previously explained, verifying the identity of a user to facilitate a transaction is a fundamental economic practice that has been performed at the point of sale well before the use of POS computers and Internet transactions. *See Elec. Commc'n Techs.*, 958 F.3d at 1182.

C

We next turn to the claims of the '826 patent. The '826 patent is entitled "Method and Apparatus for Secure Access Payment and Identification." The specification discloses a system for authenticating identities of users, including a first handheld device configured to transmit authentication information and a second device configured to receive the authentication information. '826 patent, Abstract. The first and second handheld devices are configured to wirelessly communicate with each other so that the entity associated with the first handheld device can communicate his or her identity to the entity associated with the second handheld device. *Id.* at col. 28 ll. 40–44. One embodiment of the claimed invention contemplates configuring the first handheld device so that the first entity cannot gain access to the first device without providing a PIN or biometric data (e.g., a fingerprint). *Id.* at col. 28 ll. 56–65. The second handheld device can be configured in the same manner for a second user, *id.* at col. 29 ll. 8–16, or not have a user at all, *id.* at col. 32 ll. 43–56.

Once at least the first user successfully authenticates their identity to the first handheld device, the first device may transmit a first wireless signal containing encrypted authentication information of the first user to the second device. *Id.* at col. 30 ll. 46–58. This encrypted authentication information may be

generated from biometric information received from the first handheld device, and may include generating a non-predictable signal using that biometric information. *Id.* at col. 35 ll. 22–28. For example, the signal may include multiple fields, including a digital signature field (e.g., biometric data), further identifying information (e.g., name, height, weight, eye color), and a one-time varying code field (e.g., a PKI encrypted one-time DES key). *Id.* at col. 31 l. 55–col. 32 l. 31. The second handheld device may then authenticate the first user by decrypting the authentication information and verifying the identity of the first user. *Id.* at col. 32 ll. 43–56.

Claim 10 is representative of the '826 patent claims at issue and states as follows:

> 10. A computer implemented method of authenticating an identity of a first entity, comprising acts of:
>
> authenticating, with a first handheld device, a user of the first handheld device as the first entity based on authentication information;
>
> retrieving or receiving first biometric information of the user of the first handheld device;
>
> determining a first authentication information from the first biometric information;
>
> receiving with a second device, the first authentication information of the first entity wirelessly transmitted from the first handheld device;
>
> retrieving or receiving respective second authentication information for the user of the first handheld device; and

> authenticating the identity of the first entity based upon the first authentication information and the second authentication information.

Id. at col. 45 ll. 30–47.

The district court held that the claims are "directed to the abstract idea of secured verification of a person's identity." *USR*, 469 F. Supp. 3d at 238. It reasoned that the method steps disclosed do not recite "a technological solution but instead disclose an authentication method that is accomplished by retrieving and reviewing information, including biometric information, using a handheld device and a second device, to authenticate a user's identification." *Id.* at 238–39. Further, the district court explained that the specification does not disclose "a technological solution for obtaining, generating, or analyzing biometric information, which the patent defines generically as 'any . . . method of identifying the person possessing the device.'" *Id.* at 239 (alteration in original) (quoting '826 patent col. 4 ll. 27–32).

We agree with the district court that the claims are directed to an abstract idea. Specifically, the claims are directed to multi-factor authentication of a user's identity using two devices to enable a transaction. Although USR contends that the claims cover an innovative technological solution to address problems specific to prior authentication systems, it does not proffer a persuasive argument in support of that conclusion because the claims do not include sufficient specificity. *See* Appellant's Br. 50–51. Rather, the claims generically provide for the collection of biometric information to generate a first authentication information, and then authenticating a user using both the biometric-information-derived first authen-

tication and a second authentication information. The specification even discloses that this information is conventional. *See* '826 patent col. 2 ll. 57–62 (disclosing that prior art devices use "biometric sensors that sense one or more biometric feature[s]"); *id.* at col. 1 ll. 49–53 (disclosing that prior art completes multi-factor authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"). There is no description of a specific technical solution by which the biometric information is generated, or by which the authentication information is transmitted. Because the claims broadly recite generic steps and results—as opposed to a specific solution to a technological problem—we hold that the claims are abstract under *Alice* step one. *Solutran*, 931 F.3d at 1168 (holding claims to be directed to an abstract idea "where the claims simply recite[d] conventional actions in a generic way . . . and [did] not purport to improve any underlying technology").

Turning to *Alice* step two, the district court determined that the claims do not recite "any improvements to handheld or other devices or technological solutions that enable such devices and biometric information to be combined to authenticate a user's identity remotely." *USR*, 469 F. Supp. 3d at 239. Rather, the court explained, the claims are directed to "the routine use of biometric information, mobile devices, onetime variable tokens, and/or multiple devices to authenticate a person," which "is not inventive and does not make the claimed authentication method patentable under § 101." *Id.*

We agree with the district court's conclusion that the claims do not recite an inventive concept. Rather,

the asserted claims recite well-known and conventional ways to perform authentication. *Secured Mail*, 873 F.3d at 912 (holding that the claims lacked an inventive concept where the claims recited only well-known and conventional ways to allow generic communication between a sender and recipient using generic computer technology). For example, the '826 patent explains that "the biometric information can be fingerprint information, a voiceprint, DNA codes of the first user, or any other biometric information known and used by those of skill in the art." '826 patent col. 33 ll. 22–25. The claims are likewise broad and nonspecific. Indeed, the claimed second authentication information could be anything from a social security number to a digital signature generated with a user's private PKI key. *See id.* at col. 31 l. 55–col. 32 l. 31. Thus, the claims do not recite a new authentication technique, but rather combine nonspecific, conventional authentication techniques in a non-inventive way. There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique.

D

Finally, we consider the claims of the '137 patent. The '137 patent is a continuation of the '826 patent, and similarly discloses a system for authenticating identities of users, including a first handheld device configured to transmit authentication information and a second device configured to receive the authentication information. '137 patent, Abstract. The first and second wireless devices can include a user interface with a display and a biometric sensor, where the

devices may be accessed by authenticating the user of the device using secret information (e.g., PIN number). *Id.* at col. 29 ll. 21–53.

As in the '826 patent, here an embodiment of the claimed invention contemplates the first device transmitting a first wireless signal containing encrypted authentication information of the first user to the second device. *Id.* at col. 31 ll. 19–57. This encrypted authentication information may be generated from biometric information received from the first device, and may include generating a non-predictable signal using that biometric information. *Id.* at col. 36 ll. 1–7. The second device may then authenticate the first user by decrypting the authentication information and verifying the identity of the first user. *Id.* at col. 33 ll. 20–34.

Claim 12 is a system claim and is representative of the '137 patent claims at issue:

> 12. A system for authenticating a user for enabling a transaction, the system comprising:
>
> a first device including:
>
> a biometric sensor configured to capture a first biometric information of the user;
>
> a first processor programmed to: 1) authenticate a user of the first device based on secret information, 2) retrieve or receive first biometric information of the user of the first device, 3) authenticate the user of the first device based on the first biometric, and 4) generate one or more signals including first authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value; and

> a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the one or more signals to a second device for processing;
>
> wherein generating the one or more signals occurs responsive to valid authentication of the first biometric information; and
>
> wherein the first processor is further programmed to receive an enablement signal indicating an approved transaction from the second device, wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication and use of the first authentication information and use of second authentication information to enable the transaction.

Id. at col. 46 l. 55–col. 47 l. 14.

The district court held that the claims are directed to the abstract idea of a "system for authenticating a user for enabling a transaction." *USR*, 469 F. Supp. 3d at 240 (quoting '137 patent col. 46 ll. 55–56). In reaching this conclusion, the court emphasized that the claims recite, and the specification discloses, generic well-known components—"a device, a biometric sensor, a processor, and a transceiver—performing routine functions—retrieving, receiving, sending, authenticating—in a customary order." *Id.*

Although claim 12 of the '137 patent is more detailed than claim 10 of the '826 patent, we nonetheless agree with the district court that it too is directed to an abstract idea. Claim 12 is directed to multi-factor authentication of a user's identity using two devices to enable a transaction. In particular, the claim recites

authenticating a user based on secret information, authenticating the user based on a first biometric information, and generating one or more signals including first authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value to send to a second device, where that second device will then generate an enablement signal based on the biometric authentication, the first authentication information, and second authentication information.

Though we appreciate that claim 12 of the '137 patent includes limitations not found in claim 10 of the '826 patent, the claims still are not sufficiently specific. We have previously held claims abstract "where the claims simply recite conventional actions in a generic way" without purporting to improve the underlying technology. *Solutran*, 931 F.3d at 1168; *see also McRO*, 837 F.3d at 1314 (we look to whether the claims "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" (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1326, 1336 (Fed. Cir. 2016))). This is true here. For example, claim 12 does not tell a person of ordinary skill what comprises the secret information, first authentication information, and second authentication information. While we recognize that some of the dependent claims provide more specificity on these aspects, what is claimed is still merely conventional. Indeed, the specification discloses that each authentication technique is conventional. *See* '137 patent col. 3 ll. 1–6 (disclosing that prior art devices use "biometric sensors that sense one or more biometric feature[s]"); *id.* at col. 1 ll. 60–64 (disclosing that prior art completes multi-factor

authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"); *id.* at col. 4 ll. 42–46 (disclosing that biometric information may be any of a "fingerprint, voice print, signature, iris or facial scan, or DNA analysis"); *id.* at col. 32 ll. 31–58 (disclosing that the authentication information may include "name information, a badge number, an employee number, an e-mail address, a social security number, and the like," a "digital signature" using a user's "private PKI key," and a "one-time varying code" that "includes a random code as generated by the first wireless device"); *id.* at col. 1 l. 64–col. 2 l. 3 (disclosing that known authentication software included software installed on two separate devices).

USR's assertion that this claim is akin to the claim in *Finjan* is similarly unavailing. As we explained above, the claimed invention in *Finjan* employed a new kind of file enabling a computer system to do things it could not do before, namely "behavior-based" virus scans. 879 F.3d at 1304. Here, the claimed invention merely combines conventional authentication techniques—first authentication information, a biometric authentication indicator, and a time-varying value—to achieve an expected cumulative higher degree of authentication integrity. Without some unexpected result or improvement, the claimed idea of using three or more conventional authentication techniques to achieve a higher degree of security is abstract. Likewise, as claimed in this patent, the idea of using two devices for authentication using these multiple conventional techniques is also abstract. For all these reasons, the claims are directed to an abstract idea rather than a technological solution to a technical problem.

Turning to step two, the district court determined that claim 12 "lacks the inventive concept necessary to convert the claimed system into patentable subject matter." *USR*, 469 F. Supp. 3d at 240. On appeal, USR asserts that the use of a time-varying value, a biometric authentication indicator, and authentication information that can be sent from the first device to the second device form an inventive concept. Appellant's Br. 41. We disagree. As we explained above, the specification makes clear that each of these devices and functions is conventional. *See supra* at 24–25. Further, we conclude that adding them all together is itself directed to the conventional idea of multi-factor authentication. USR further asserts that authenticating a user at two locations constitutes an inventive concept because it is locating the authentication functionality at a specific, unconventional location within the network. Appellant's Br. 41 (citing *BASCOM*, 827 F.3d at 1350). Unlike the claims in *BASCOM*, however, the specification suggests that the claims here only recite a conventional location for the authentication functionality. *See* '137 patent col. 1 ll. 60–64 (disclosing that prior art completes multi-factor authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"). Thus, nothing in the claims is directed to a new authentication technique; rather, the claims are directed to combining longstanding, known authentication techniques to yield expected additory amounts of security. There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the combination of these conventional authentication techniques results in an unexpected improvement

beyond the expected sum of the security benefits of each individual authentication technique.

CONCLUSION

We have considered USR's remaining arguments and find them unpersuasive. For the foregoing reasons, we affirm the district court's decision to dismiss, as the asserted patents claim unpatentable subject matter.

AFFIRMED

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

Civ. No. 17-585-CFC-SRF

UNIVERSAL SECURE REGISTRY LLC,

Plaintiff,

v.

APPLE INC., VISA INC., and VISA U.S.A. INC.,

Defendants.

June 30, 2020
Wilmington, Delaware

MEMORANDUM OPINION

Jack B. Blumenfeld and Jeremy A. Tigan, Morris, Nichols, Arsht & Tunnell LLP, Wilmington, DE. Harold Barza, Tigran Guledjian, Valerie Roddy, and Jordan Kaericher, Quinn Emanuel Urquhart & Sullivan, LLP, Los Angeles, CA. Sean Pak and Brian E. Mack, Quinn Emanuel Urquhart & Sullivan, LLP, San Francisco, CA. *Attorneys for Universal Secure Registry LLC.*

David E. Moore and Bindu Palapura, Potter Anderson & Corroon LLP, Wilmington, DE. James C. Yoon, Jamie Y. Otto, and Jacqueline Lyandres, Wilson Sonsini Goodrich & Rosati, Palo Alto, CA. Lucy Yen,

Wilson Sonsini Goodrich & Rosati, New York, NY. Ian Liston, Wilson Sonsini Goodrich & Rosati, Wilmington, DE. *Attorneys for Defendants Visa Inc. and Visa U.S.A., Inc.*

Frederick L. Cottrell, III and Jason J. Rawnsley, Richards, Layton & Finger, P.A., Wilmington, DE. Mark D. Selwyn and Liv Herriot, Wilmer Cutler Pickering Hale and Dorr LLP, Palo Alto, CA. Monica Grewal, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA. Derek A. Gosma, Wilmer Cutler Pickering Hale and Dorr LLP, Los Angeles, CA. *Attorneys for Defendant Apple Inc.*

/s/ Colm F. Connolly
CONNOLLY, United States District Judge

Plaintiff Universal Secure Registry LLC (USR) has sued Defendants Apple Inc., Visa Inc., and Visa U.S.A., Inc. for infringement of U.S. Patent Nos. 8,856,539 (the #539 patent), 9,100,826 (the #826 patent), 8,577,813 (the #813 patent), and 9,530,137 (the #137 patent). Defendants moved to dismiss the Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6) on the grounds that the asserted patents claim unpatentable subject matter and are therefore invalid under 35 U.S.C. § 101. D.I. 16. In a Report and Recommendation issued pursuant to 28 U.S.C. § 636(b), the Magistrate Judge recommended that I deny Defendants' motion. D.I. 137.

Pending before me are Defendants' objections to the Magistrate Judge's recommendation. D.I. 147. I have studied the Report and Recommendation, the objections, Plaintiff's response to the objections, D.I. 150, and the parties' briefs filed in support and opposition to the underlying motions, D.I. 17, D.I. 30,

D.I. 37. I review the Magistrate Judge's recommendation de novo. § 636(b)(1); Fed. R. Civ. P. 72(b)(3).

I. BACKGROUND

The four asserted patents are directed to the secure authentication (i.e., verification) of a person's identity. In the words of the Complaint: "USR's patented innovations allow a user to securely authenticate his or her identity using technology built into a personal electronic device combined with the user's own secret and/or biometric information." D.I. 1 ¶ 21.

USR alleged in the Complaint that each patent has an "exemplary" claim. D.I. 1 ¶¶ 43, 65, 84, 106. Exemplary claim 22 of the #539 patent provides:

> A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multi character code, the method comprising:
>
> receiving a transaction request including at least the time varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;
>
> mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;
>
> determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;

> accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;
>
> providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction; and
>
> enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information.

#539 patent at 20:4-31.

Exemplary claim 10 of the #826 patent provides:

> A computer implemented method of authenticating an identity of a first entity, comprising acts of:
>
> authenticating, with a first handheld device, a user of the first handheld device as the first entity based on authentication information;
>
> retrieving or receiving first biometric information of the user of the first handheld device;
>
> determining a first authentication information from the first biometric information;
>
> receiving with a second device, the first authentication information of the first entity wirelessly transmitted from the first handheld device;
>
> retrieving or receiving respective second authentication information for the user of the first handheld device; and

> authenticating the identity of the first entity based upon the first authentication information and the second authentication information.

#826 patent at 45:30-47.

Exemplary claim 1 of the #813 patent, which has been reformatted for clarity, provides:

> An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> a biometric sensor configured to receive a biometric input provided by the user;
>
> a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;
>
> a communication interface configured to communicate with a secure registry;
>
> a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface,
>
> > the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information,
> >
> > the processor also being programmed such that once the electronic ID device is

> activated the processor is configured to generate a nonpredictable value and to generate encrypted authentication information from the nonpredictable value, information associated with at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and
>
> wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and
>
> wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

#813 patent at 51:65-29.

Finally, exemplary claim 12 of the #137 patent provides:

> A system for authenticating a user for enabling a transaction, the system comprising:
>
> a first device including:
>
> a biometric sensor configured to capture a first biometric information of the user;
>
> a first processor programmed to: 1) authenticate a user of the first device based on secret information, 2) retrieve or receive first biometric information of the user of the first device, 3) authenticate the user of the first device based on the first biometric, and 4) generate one or more signals including first

> authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value; and
>
> a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the one or more signals to a second device for processing;
>
> wherein generating the one or more signals occurs responsive to valid authentication of the first biometric information; and
>
> wherein the first processor is further programmed to receive an enablement signal indicating an approved transaction from the second device,
>
> wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication and use of the first authentication information and use of second authentication information to enable the transaction.

#137 patent at 46:55-47:14.

Defendants argue that these exemplary claims are directed to an abstract idea and therefore claim unpatentable subject matter under § 101. The Magistrate Judge found that the patents are "not directed to an abstract idea because 'the plain focus of the claims is on an improvement to computer functionality, not on economic or other tasks for which a computer is used in its ordinary capacity.'" D.I. 137 at 18, 19, 21, 23 (quoting *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017)).

II. LEGAL STANDARDS

A. Rule 12(b)(6)

To state a claim on which relief can be granted, a complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Detailed factual allegations are not required, but the complaint must include more than mere "labels and conclusions" or "a formulaic recitation of the elements of a cause of action." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citation omitted). The complaint must set forth enough facts, accepted as true, to "state a claim to relief that is plausible on its face." *Id.* at 570. A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). Deciding whether a claim is plausible is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* at 679 (citation omitted).

B. Patent-Eligible Subject Matter

Section 101 of the Patent Act defines patent-eligible subject matter. It provides: "Whoever 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.

There are three judicially created limitations on the literal words of § 101. The Supreme Court has long held that laws of nature, natural phenomena, and abstract ideas are not patentable subject matter. *Alice*

Corp. Pty. v. CLS Bank Int'l, 573 U.S. 208, 216 (2014). These exceptions to patentable subject matter arise from the concern that the monopolization of "the[se] basic tools of scientific and technological work" "might tend to impede innovation more than it would tend to promote it." *Id.* (internal quotation marks and citations omitted).

"[A]n invention is not rendered ineligible for patent [protection] simply because it involves an abstract concept." *Alice*, 573 U.S. at 217. "Applications of such concepts to a new and useful end . . . remain eligible for patent protection." *Id.* (internal quotation marks, alterations, and citations omitted). But "to transform an unpatentable law of nature [or abstract idea] into a patent-eligible application of such a law [or abstract idea], one must do more than simply state the law of nature [or abstract idea] while adding the words 'apply it.'" *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72 (2012) (emphasis removed).

In *Alice*, the Supreme Court established a two-step framework by which courts are to distinguish patents that claim eligible subject matter under § 101 from patents that do not claim eligible subject matter under § 101. The court must first determine whether the patent's claims are drawn to a patent-ineligible concept—i.e., are the claims directed to a law of nature, natural phenomenon, or abstract idea? *Alice*, 573 U.S. at 217. If the answer to this question is no, then the patent is not invalid for teaching ineligible subject matter. If the answer to this question is yes, then the court must proceed 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) (internal quotations and citations omitted).

III. DISCUSSION

I agree with Defendants that the exemplary claims of the asserted patents do not recite patentable subject matter. The patents are directed to an abstract idea — the secure verification of a person's identity—and therefore fail step one of the *Alice* inquiry. And the patents do not disclose an inventive concept such as an improvement in computer functionality that transforms that abstract idea into a patent-eligible application of the idea.

The Magistrate Judge found that the patents are not directed to an abstract idea based on her finding that the asserted exemplary claims teach improvements in computer functionality. USR, however, has never argued that the patents disclose improvements in computer technology; and, in my view, neither the patents' claims nor their written descriptions teach or purport to teach improvements in computer functionality. Moreover, contrary to USR's arguments, neither the patents nor their written descriptions disclose "concrete and useful improvements" to "technical challenges associated with digital security and authentication" that transform the subject matter of the claims patentable under § 101. D.I. 30 at 2-3.

A. Claim 22 of the #539 Patent

As its preamble acknowledges, claim 22 teaches "[a] method for providing information to a provider [typically, a merchant] to enable transactions between the provider and entities [typically, a customer of the

merchant] who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code." In other words, it teaches a method to obtain the secure verification of a person's identity to enable a commercial transaction.

The #539 patent is not materially different from the patent at issue in *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014 (Fed. Cir. 2017). The Federal Circuit determined that the patent in *Prism Tech.* was invalid because it was directed to the abstract idea of "providing restricted access to resources." *Id.* at 1016-17. The claims of the patent in *Prism Tech.* taught "an abstract process" that included: "(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources." *Id.* The #539 patent's authentication method closely parallels this abstract process. Claim 22 of the #539 patent teaches: (1) "receiving" a transaction request with a time-varying multicharacter code and "an indication of" the merchant requesting the transaction; (2) "mapping" the time-varying multicharacter code to the identity of the customer in question; (3) "determining" whether the merchant's access to the customer's secure data complies with any restrictions; (4) "accessing" the customer's account information; (5) "providing" the account identifying information to a third party without providing that information to the merchant; and (6) "enabling or denying" the merchant to perform the transaction without obtaining knowledge of the customer's identifying information. #539 patent at 20:4-32. Given the similarities between these six steps and the claimed process in *Prism Tech.*, I find

that claim 22 is directed to the abstract idea of obtaining the secure verification of a user's identity to enable a transaction.

Turning to step two of the analysis, as the patent itself acknowledges, all of the steps to the claimed process are accomplished by implementing well-known methods using conventional computer components. *See* #539 patent at 5:63-66 ("The computer system may be a general purpose computer . . . ."); 6:4-7:10 ("In a general purpose computer system, the processor is typically a commercially available microprocessor," "The database 24 may be any kind of database," etc.). The claimed process therefore fails step two. *See Alice*, 573 U.S. at 222-23, 225 (considering at step two "the introduction of a computer into the claims" and holding that the use of "a generic computer to perform generic computer functions" does not provide the requisite inventive concept to satisfy step two); *Prism Tech*., 696 F. App'x at 1017-18 (holding that, "[v]iewed as an ordered combination, the asserted claims recite[d] no more than the sort of 'perfectly conventional' generic computer components employed in a customary manner" that did "not rise to the level of an inventive concept" and therefore did not "transform the abstract idea into a patent-eligible invention" under *Alice* step two).[1]

---

[1] I recognize that the Federal Circuit has on other occasions considered computer functionality as part of step one of the *Alice* inquiry. *See, e.g., Enfish, LLC v. Microsoft Corp.,* 822 F.3d 1327, 1335-36 (Fed. Cir. 2016) (considering introduction of computer functionality into claims as part of step one of *Alice* inquiry); *see also In re TLI Commc'ns LLC Patent Litig.,* 823 F.3d 607, 611-13 (Fed. Cir. 2016) (same). Whether computer functionality is considered at step one or step two seems to me immaterial as long as it is considered at some point in the *Alice* analysis.

USR argues that the "key" to claim 22's innovation is "allow[ing] transaction approval ***without providing account identifying information to the merchant.***" D.I. 30 at 19 (emphasis in original). But sending data to a third-party as opposed to the merchant is not a technological innovation, but rather a "insignificant post-solution activity" that is insufficient to confer patent eligibility. *Bilski v. Kappos*, 561 U.S. 593, 611 (2010).

USR also intimates that the use of a time-varying code provides an inventive concept. D.I. 30 at 19. But the claimed method employs the use of a time-varying code in a customary manner and in the naturally expected order of steps. *See Boom! Payments, Inc. v. Stripe, Inc.*, 2019 WL 6605314, at *1 (N.D. Cal. Nov. 19, 2019) (claims directed to "authenticating internet sales through use of a third party intermediary" lack an inventive concept where "[a] third-party server receives and stores the buyer's payment information," the server "generates and sends a transaction-specific code to the buyer," "the buyer sends the code to the seller," the seller "sends the code (and identifying information) to the server," and "[i]f the code is a match, the server processes the payment"); *Asghari-Kamrani v. United Serv. Auto. Ass'n*, 2016 WL 3670804, at *5-6 (E.D. Va. July 5, 2016) (claims verifying the identity of a participant to a transaction using a randomly generated code lack an inventive concept where the steps include (1) "receiving" a request for a dynamic code at a central entity; (2) "generating" a dynamic code by the central entity; (3) "providing" the generated dynamic code to the user; (4) "receiving" a request for authenticating the user from an external entity; and (5) "authenticating" by the central entity the user and providing the result to the external entity"); *Inventor Holdings, LLC v. Bed Bath &*

Beyond Inc., 123 F.Supp.3d 557, 562 (D. Del. 2015) (claim for processing a payment for a purchase of goods lacks an inventive concept where the steps include "(a) receiving a code relating to a purchase of goods; (b) determining if the code relates to a local or remote order; and (c) if the code is for a remote order, then determining the price, receiving payment, and alerting the remote seller that payment has been received").

B. Claim 10 of the #826 Patent

As with claim 1 of the #539 patent, the preamble of claim 10 of the #826 patent makes clear that claim 10's method is directed to the abstract idea of secured verification of a person's identity. The preamble reads: "[a] computer implemented method of authenticating an identity of a first entity[.]" #826 patent at 45:30-31. The six method steps disclosed in the remainder of claim 10 do not teach a technological solution but instead disclose an authentication method that is accomplished by retrieving and reviewing information, including biometric information, using a handheld device and a second device, to authenticate a user's identification.

USR argues that the claimed method is not abstract and teaches inventive "technological improvements over prior art systems" because it "include[es]: (1) gathering biometric information while locally authenticating the user, preventing unauthorized use of the device; and (2) requiring additional remote user authentication by a second device, based on both authentication information (e.g., one-time variable token) received from the first device, and second authentication information (e.g., information securely stored at the second device or obtained from the [Universal Secure Registry database])." D.I. 30 at 15.

But the patent does not teach a technological solution for obtaining, generating, or analyzing biometric information, which the patent defines generically as "any . . . method of identifying the person possessing the device." #826 patent at 4:27-32. Nor does the patent teach any improvements to handheld or other devices or technological solutions that enable such devices and biometric information to be combined to authenticate a user's identity remotely. Rather, the patent teaches the routine use of biometric information, mobile devices, onetime variable tokens, and/or multiple devices to authenticate a person. That teaching is not inventive and does not make the claimed authentication method patentable under § 101. *See IQS US Inc. v. Calsoft Labs Inc.*, 2017 WL 3581162, at *5 (N.D. Ill. Aug. 18, 2017) (patent using generic functions of existing technology to verify identity based on biometric information lacked an inventive concept); *Intellectual Ventures I LLC v. Erie Indem. Co.*, 850 F.3d 1315, 1331 (Fed. Cir. 2017) (patent implementing mobile interface in generic manner to access user's data lacked an inventive concept); *Boom!*, 2019 WL 6605314, at *1 ("generat[ing] and sending] a transaction-specific code to the buyer" lacks an inventive concept because it is a generic computer function); *Asghari-Kamrani*, 2016 WL 3670804, at *5 ("generating a random code" is a "conventional computer function[]" that lacks an inventive concept); *Smart Authentication IP, LLC v. Elec. Arts Inc.*, 402 F. Supp. 3d 842, 853 (N.D. Cal. 2019) ("Using well-known computer technology to authenticate a user – even using multiple electronic media to do so – amounts to functional use of familiar technology and is not inventive.").

C. Claim 1 of the #813 Patent

USR argues that the Electronic ID Device disclosed in claim 1 of the #813 patent "includes a biometric sensor, user interface, communication interface, and processor, all working together in a specific way to generate and transmit encrypted authentication information via a [point-of-sale] device to a secure registry." D.I. 30 at 5. But the patent does not disclose a specific technical solution by which such encrypted information is generated or transmitted. Rather, as USR states in its briefing, the patent merely discloses that "[t]he Electronic ID Device collects biometric information from the user, secret information known by the user, and account identifying information selected by the user to activate the device, and to generate a non-predicable value and the encrypted authentication information." *Id.* In other words, the device collects and examines data to authenticate the user's identity.

The patent describes the Electronic ID Device as "any type of electronic device" capable of accessing a secure identification system database, #813 patent at 13:5-8, and it describes the device as consisting of well-known, generic components, including a computer processor, *see id.* at 5:30-34, 7:1-7, 27:25-29, 43:21-33, 50:3-11. Accordingly, it does not teach an inventive concept that transforms the abstract idea of authenticating identity into patentable subject matter. *See In re Gopalan*, 2020 WL 1845308, at *4 (Fed. Cir. Apr. 13, 2020) (holding that performing the steps of an abstract concept "on a generic processor does not transform it into a patentable apparatus").

D. Claim 12 of the #137 Patent

The preamble of claim 12 of the #137 patent states that the claim is directed to "[a] system for authen-

ticating a user for enabling a transaction." #137 patent at 46:55-56. The system disclosed to accomplish this abstract task is comprised of generic components—a device, a biometric sensor, a processor, and a transceiver—performing routine functions retrieving, receiving, sending, authenticating—in a customary order. *Prism Tech*., 696 F. App'x at 1017; *Telesign Corp. v. Twilio, Inc*., 2018 WL 10638619, at *2 (N.D. Cal. Oct. 19, 2018). Accordingly, it lacks the inventive concept necessary to convert the claimed system into patentable subject matter. *Alice*, 573 U.S. at 222-23, 225; *Prism Tech.*, 696 F. App'x at 1017-18.

IV. CONCLUSION

For the foregoing reasons, I will not adopt the recommendation of the Magistrate Judge and will instead grant Defendants' motion to dismiss the Complaint for failure to state a claim.

The Court will issue an Order consistent with this Memorandum Opinion.

APPENDIX C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

[Filed September 19, 2018]

Civil Action No. 17-585-CFC-SRF

UNIVERSAL SECURE REGISTRY, LLC,

Plaintiff,

v.

APPLE INC., VISA INC., and VISA U.S.A., INC.,

Defendants.

REPORT AND RECOMMENDATION

I. INTRODUCTION

Presently before the court in this patent infringement action are the following motions: (1) a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to Federal Rule of Civil Procedure 12(b)(6), filed by defendants Apple Inc., Visa Inc., and Visa U.S.A., Inc. (collectively "defendants") (D.I. 16); and (2) defendants' motion to transfer venue to the Northern District of California pursuant to 28 U.S.C. § 1404 (D.I. 21). For the following reasons, I recommend that the court deny defendants' motions to dismiss and transfer.

II. BACKGROUND

A. Parties

Plaintiff Universal Secure Registry, LLC ("USR") is a limited liability company organized and existing

under the laws of Massachusetts with its principal place of business in Newton, Massachusetts. (D.I. 1 at ¶ 4) USR develops technological solutions for identity authentication, computer security, and digital and mobile payment security which allow users to securely authenticate their identity using technology built into a personal electronic device combined with the users' biometric information. (*Id.* at ¶ 21) USR is the owner by assignment of United States Patent Nos. 8,577,813 ("the '813 patent"); 8,856,539 ("the '539 patent"); 9,100,826 ("the '826 patent"); and 9,530,137 ("the '137 patent") (collectively, the "patents-in-suit"). (*Id.* at ¶¶ 2-3) The patents-in-suit allow a user to employ an electronic device as an "electronic wallet" capable of interacting with point-of-sale devices to authorize payments. (*Id.* at ¶ 22)

Apple Inc. ("Apple") is incorporated in California and maintains its headquarters in Cupertino in the Northern District of California. (*Id.* at ¶ 5) Apple maintains a retail store in Delaware. (*Id.* at ¶ 13) Visa Inc. and Visa U.S.A., Inc. ("Visa") are Delaware corporations maintaining a principal place of business in Foster City, California. (*Id.* at ¶¶ 6-7) USR accuses defendants of infringing the patents-in-suit by providing the Apple Pay service. (*Id.* at ¶¶ 8-9) Specifically, USR identifies the following allegedly infringing devices which support Apple Pay:

> Apple iPhone 7, iPhone 7 Plus, iPhone 6s, iPhone 6s Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5, 5s, and 5c (paired with Apple Watch), iPad (5th generation), iPad Pro (12.9 inch), iPad Pro (9.7 inch), iPad Air 2, iPad mini 4, iPad mini 3, Apple Watch Series 2, Apple Watch Series 1, Apple Watch (1st generation), MacBook Pro with Touch ID, and

> all Mac models introduced in 2012 or later (with an Apple Pay-enabled iPhone or Apple Watch) (collectively, the "Accused Products")
> . . . .

(*Id.* at ¶ 39)

B. Patents-In-Suit

USR filed this patent infringement action on May 21, 2017, asserting claims for infringement regarding the patents-in-suit. (D.I. 1 at ¶ 2) The '813 and '539 patents are both entitled "Universal Secure Registry" and list Dr. Kenneth P. Weiss as the sole inventor. (*Id.* at ¶¶ 25-26) The '813 patent issued on November 5, 2013, and the '539 patent was granted on October 7, 2014. (*Id.*) The '826 and '137 patents are both entitled "Method and Apparatus for Secure Access Payment and Identification," and list Dr. Weiss as the sole inventor. (*Id.* at ¶¶ 27-28) The '826 patent issued on August 14, 2015, and the '137 patent issued on December 27, 2016. (*Id.*)

C. Procedural History

In 2010, USR sent Apple multiple letters describing its patented technology and seeking to partner with Apple to jointly develop a payment method involving a software-modified payment phone and the use of biometric identity authentication. (D.I. 1 at ¶ 33) USR also pursued a partnership with Visa during this time, engaging in a series of confidential discussions with senior Visa representatives which included detailed presentations of the patented technology under the protection of a non-disclosure agreement. (*Id* at ¶ 34) Instead of partnering with USR, Apple and Visa ultimately partnered with each other and other payment networks and banks as early as January 2013 to allegedly incorporate the patented technology into the Apple

Pay service. (*Id.* at ¶ 35) Apple publicly launched Apple Pay on September 9, 2014. (*Id.* at ¶ 36)

III. DISCUSSION

A. Venue

1. Legal standard

Section 1404(a) of Title 28 of the United States Code grants district courts the authority to transfer venue "[f]or the convenience of parties and witnesses, in the interests of justice . . . to any other district or division where it might have been brought." 28 U.S.C. § 1404(a). Much has been written about the legal standard for motions to transfer under 28 U.S.C. § 1404(a). *See, e.g., In re Link A_Media Devices Corp.,* 662 F.3d 1221 (Fed. Cir. 2011); *Jumara v. State Farm Ins. Co.,* 55 F.3d 873 (3d Cir. 1995); *Helicos Biosciences Corp. v. Illumina, Inc.,* 858 F. Supp. 2d 367 (D. Del. 2012).

Referring specifically to the analytical framework described in *Helicos,* the court starts with the premise that a defendant's state of incorporation has always been "a predictable, legitimate venue for bringing suit" and that "a plaintiff, as the injured party, generally ha[s] been 'accorded [the] privilege of bringing an action where he chooses.' 858 F. Supp. 2d at 371 (quoting *Norwood v. Kirkpatrick,* 349 U.S. 29, 31 (1955)). Indeed, the Third Circuit in *Jumara* reminds the reader that "[t]he burden of establishing the need for transfer . . . rests with the movant" and that, "in ruling on defendants' motion, the plaintiff's choice of venue should not be lightly disturbed." 55 F.3d at 879 (citation omitted).

The Third Circuit goes on to recognize that,

> [i]n ruling on § 1404(a) motions, courts have not limited their consideration to the three

> enumerated factors in § 1404(a) (convenience of parties, convenience of witnesses, or interests of justice), and, indeed, commentators have called on the courts to "consider all relevant factors to determine whether on balance the litigation would more conveniently proceed and the interests of justice be better served by transfer to a different forum."

Id. (citation omitted). The Court then describes some of the "many variants of the private and public interests protected by the language of § 1404(a)." *Id.*

> The private interests have included: plaintiff's forum of preference as manifested in the original choice; the defendant's preference; whether the claim arose elsewhere; the convenience of the parties as indicated by their relative physical and financial condition; the convenience of the witnesses – but only to the extent that the witnesses may actually be unavailable for trial in one of the fora; and the location of books and records (similarly limited to the extent that the files could not be produced in the alternative forum).
>
> The public interests have included: the enforceability of the judgment; practical considerations that could make the trial easy, expeditious, or inexpensive; the relative administrative difficulty in the two fora resulting from court congestion; the local interest in deciding local controversies at home; the public policies of the fora; and the familiarity of the trial judge with the applicable state law in diversity cases.

Id. (citations omitted).

Considering these "jurisdictional guideposts," the court turns to the "difficult issue of federal comity" presented by transfer motions. *E.E.O.C. v. Univ. of Pa.,* 850 F.2d 969, 976 (3d Cir. 1988). USR has not challenged defendants' assertion that venue would also be proper in the Northern District of California. (D.I. 31 at 3) As such, the court does not further address the appropriateness of the proposed transferee forum.[1] *See* 28 U.S.C. § 1404(a).

2. Private Interests

(a) Plaintiffs forum preference

Plaintiffs have historically been accorded the privilege of choosing their preferred venue for pursuing their claims. *See C. R. Bard, Inc. v. AngioDynamics, Inc.,* 156 F. Supp. 3d 540, 545 (D. Del. 2016). "It is black letter law that a plaintiff's choice of a proper forum is a paramount consideration in any determination of a transfer request, and that choice 'should not be lightly disturbed.'" *Shuttle v. Armco Steel Corp.,* 431 F.2d 22, 25 (3d Cir. 1970) (internal citation omitted). However, the Federal Circuit has recognized that "[w]hen a plaintiff brings its charges in a venue that is not its home forum . . . that choice of forum is entitled to less deference, *In re Link A_Media Devices Corp.,* 662 F.3d 1221, 1223 (Fed. Cir. 2011), and judges within this district have defined a party's "home forum" as its principal place of business, *see Mitel Networks Corp. v. Facebook, Inc.,* 943 F. Supp. 2d 463, 469-70 (D. Del. 2013).

---

[1] The first step in the transfer analysis is to determine whether the movant has demonstrated that the action could have been brought in the proposed transferee venue in the first instance. *See Mallinckrodt, Inc. v. E-Z-Em, Inc.,* 670 F. Supp. 2d 329, 356 (D. Del. 2009). This issue is not disputed. (D.I. 31 at 3)

In the present action, USR does not allege that it has facilities, employees, or operations in Delaware. USR's choice of Delaware as a forum weighs in USR's favor, but not as strongly as it would if USR had a place of business in Delaware. *See IpVenture, Inc. v. Acer, Inc.,* 879 F. Supp. 2d 426, 431 (D. Del. 2012); *see also Symantec Corp. v. Zscaler, Inc.,* C.A. No. 17-806-MAK, D.I. 25 at 3-4 (D. Del. July 31, 2017) (citing *Memory Integrity, LLC v. Intel Corp.,* C.A. No. 13-1804-GMS, 2015 WL 632026, at *3 (D. Del. Feb. 13, 2015) (concluding that a non-practicing entity's choice of forum should receive limited deference because it had no physical presence in Delaware)). Consequently, USR's forum preference weighs slightly against transfer.

(b) Defendant's forum preference

Defendants' preference to litigate in the Northern District of California, where defendants maintain their principal places of business, weighs in favor of transferring venue. However, defendants' preference is accorded less weight than USR's preference. *See Stephenson v. Game Show Network, LLC,* 933 F. Supp. 2d 674, 678 (D. Del. 2013) (citing *Cradle IP, LLC v. Texas Instruments, Inc.,* 923 F. Supp. 2d 696, 699-700 (D. Del. 2013)).

(c) Where the claim arose

A claim for patent infringement arises wherever someone has committed acts of infringement. *See generally* 35 U.S.C. § 271(a); *Red Wing Shoe Co., Inc. v. HockersonHalberstadt, Inc.,* 148 F.3d 1355, 1360 (Fed. Cir. 1998) (an infringement claim "arises out of instances of making, using, or selling the patented invention"). Because defendants' allegedly infringing products are sold and used nationwide, the asserted patent claims may be said to arise in Delaware. *See*

C. R. Bard, Inc. v. AngioDynamics, Inc., 156 F. Supp. 3d 540, 547 (D. Del. 2016) (finding that a patent claim arose in Delaware when the defendant sold products there); *Scientific Telecomm., LLC v. Adtran, Inc.,* C.A. No. 15-647-SLR, 2016 WL 1650760, at *1 (D. Del. Apr. 25, 2016) (holding that, despite ties to Alabama, the defendant operated on a global basis, and its incorporation in Delaware precluded arguments that the forum was inconvenient absent a showing of a unique or unexpected burden). This factor is neutral.

(d) Convenience of the parties

In evaluating the convenience of the parties, a district court should focus on the parties' relative physical and financial condition. *See C. R. Bard,* 2016 WL 153033, at *3 (citing *Jumara v. State Farm Ins. Co.,* 55 F.3d 873, 879 (3d Cir. 1995)). When a party "accept[s] the benefits of incorporation under the laws of the State of Delaware, 'a company should not be successful in arguing that litigation' in Delaware is 'inconvenient,' 'absent some showing of a unique or unexpected burden.'" *Scientific Telecomm., LLC v. Adtran, Inc.,* C.A. No. 15-647-SLR, 2016 WL 1650760, at *1 (D. Del. Apr. 25, 2016) (quoting *ADE Corp. v. KLA-Tencor Corp.,* 138 F. Supp. 2d 565, 573 (D. Del. 2001)). "Unless the defendant 'is truly regional in character' – that is, it operates essentially exclusively in a region that does not include Delaware – transfer is almost always inappropriate." *Checkpoint,* 797 F. Supp. 2d at 477 (quoting *Praxair, Inc. v. ATMI, Inc.,* 2004 WL 883395, at *1 (D. Del. Apr. 20, 2004)).

The record before the court reveals that USR is a small company with negative cash flow and no income, funded out of the savings of its founder, Dr. Weiss. (D.I. 36 at ¶ 11) The USR entities collectively have six full-time employees, two part-time employees, and

three consultants located in Massachusetts. (*Id.* at ¶ 9) USR's records are kept in six storage boxes in Massachusetts. (*Id.* at ¶ 10) In contrast, there is no dispute that Apple and Visa are large, wealthy corporations who engage in business throughout the United States. (D.I. 38 at 6) Defendants have not shown a unique or unexpected burden as required to support transfer under the relevant standard. *See Cornerstone Therapeutics Inc. v. Exela Pharma Scis., LLC,* C.A. No. 13-1275-GMS, 2014 WL 12597625, at *1 (D. Del. June 16, 2014) ("[T]he decision of two out of three defendants to incorporate in Delaware casts doubt on their arguments that litigating in this state is inconvenient.").

Defendants point out that USR has no connections to Delaware, yet has accepted the costs of travel to Delaware by choosing to litigate here. (D.I. 22 at 15) (quoting *Blackbird Tech LLC v. TuffStuff Fitness, International, Inc.,* C.A. No. 16-733-GMS, 2017 WL 1536394, at *5 (D. Del. Apr. 27, 2017) ("The court believes that Blackbird, given its location, structure of its company, and lack of substantial connections in Delaware, would suffer little added inconvenience were this case transferred away from its preferred forum.")). However, the distance between Massachusetts and the Northern District of California is substantially greater than the distance between Massachusetts and Delaware. Focusing on the significant difference in the parties' relative financial positions, as well as USR's proximity to Delaware in comparison to the Northern District of California, the court concludes that the

present record does not support transfer of venue.[2] This factor weighs slightly against transfer.

(e) Location of books and records

The Third Circuit in *Jumara* advised that the location of books and records is only determinative if "the files c[an] not be produced in the alternative forum." 55 F.3d at 879. However, the Federal Circuit has explained that "[i]n patent infringement cases, the bulk of the relevant evidence usually comes from the accused infringer. Consequently, the place where the defendant's documents are kept weighs in favor of transfer to that location." *In re Genentech, Inc.,* 566 F.3d 1338, 1345 (Fed. Cir. 2009). Nevertheless, courts within the District of Delaware have repeatedly recognized that technological advances have reduced the weight of this factor. *See, e.g., Intellectual Ventures I LLC, v. Checkpoint Software Techs. Ltd.,* 797 F. Supp. 2d 472, 485 (D. Del. 2011); *Affymetrix, Inc. v. Synteni, Inc.,* 28 F. Supp. 2d 192, 208 (D. Del. 1998); *Nihon Tsushin Kabushiki Kaisha v. Davidson,* 595 F. Supp. 2d 363, 372 (D. Del. 2009). Today, "virtually all businesses maintain their books and records in electronic format readily available for review and use at any location." *C.R. Bard,* 2016 WL 153033, at *3; *see also Quest Integrity USA, LLC v. Clean Harbors Indus. Servs., Inc.,* 114 F. Supp. 3d 187, 191 (D. Del. 2015).

---

[2] The court recognizes that the analysis of this factor typically focuses on the size and financial position of the defendant, as opposed to the plaintiff, given that the defendant does not choose to commence the litigation. Nonetheless, the disparity between the parties' size and financial condition is evident in the instant case, and litigating in the Northern District of California is likely to be more expensive and burdensome for USR.

Defendants designed and developed the allegedly infringing technology in the Northern District of California, and much of the documentary evidence is located there. (D.I. 23 at ¶¶ 7-9) Defendants have not shown that relevant documents cannot be transported to Delaware. *See Cruise Control Techs. LLC v. Chrysler Group LLC,* C.A. No. 12-1755-GMS, 2014 WL 1304820, at *4 (D. Del. Mar. 31, 2014) (concluding that location of books and records is only relevant "where the Defendants show that there are books and records that cannot be transported or transmitted to Delaware."). This factor weighs slightly in favor of transfer.

(f) Convenience of the witnesses

The relevant inquiry with respect to convenience of the witnesses is not whether witnesses are inconvenienced by litigation, but rather, whether witnesses "actually may be unavailable for trial in one of the fora." *Jumara,* 55 F.3d at 879. The inconvenience of travel does not demonstrate that witnesses would "actually be unavailable for trial," as required by *Jumara.* 55 F.3d 873, 879 (3d Cir. 1995). The court has previously found that

> travel expenses and inconveniences incurred for that purpose, by a Delaware defendant, [are] not overly burdensome. From a practical standpoint, much of the testimony presented at trial these days is presented via recorded depositions, as opposed to witnesses traveling and appearing live. There certainly is no obstacle to [a party] embracing this routine trial practice.

Oracle Corp. v. epicRealm Licensing, LP, No. Civ. 06-414-SLR, 2007 WL 901543, at *4 (D. Del. Mar. 26, 2007).

Defendants identify six prior art witnesses who reside in or near the Northern District of California and are named inventors on patent applications. (D.I. 24 at ¶ 13) Defendants do not identify former employees or other third party witnesses. Other third party witnesses involved in the prosecution of the patents-in-suit are located in Massachusetts and have affirmatively expressed their willingness to testify at trial in Delaware, despite residing beyond the subpoena power of both this court and the proposed transferee district. (D.I. 32 at ¶¶ 3-6; D.I. 34 at ¶¶ 3-6) An independent technology consultant to USR residing in Massachusetts also indicated that he will voluntarily travel to Delaware to testify at trial in this matter. (D.I. 33 at ¶¶ 2-5) Because defendants have not identified any specific witnesses who cannot appear in Delaware for trial, this factor is neutral.

3. Public interests[3]

(a) Practical considerations

Defendants reiterate their arguments regarding private interest factors such as the convenience of the parties and witnesses, and the location of evidence, in support of their position on practical considerations. (D.I. 22 at 18) Courts in this district have declined to "double-count" a defendant's arguments in such cases. *Contour IP Holding, LLC v. GoPro, Inc.,* C.A. No. 15-1108-LPS-CJB, 2017 WL 3189005, at *13 (D. Del. July 6, 2017). This factor is neutral.

---

[3] Turning to the *Jumara* factors, the court notes that the parties do not dispute several of the public interest factors: (1) the enforceability of the judgment; (2) the public policies of the fora; and (3) the familiarity of the trial judge with the applicable state law in diversity cases. (D.I. 22 at 17-20; D.I. 31 at 15-19) These factors are therefore neutral.

(b) Court congestion

Defendants allege that this factor weighs in favor of transfer due to the judicial vacancies on this court, citing statistics[4] regarding the number of open patent cases and the rates at which new patent cases are filed in each jurisdiction. (D.I. 22 at 18-19; D.I. 38 at 10) However, "the case management orders [in this district] always start with the schedules proposed by the litigants . . . . [I]f there is a need to expedite proceedings, that need is generally accommodated by the court." *Godo Kaisha IP Bridge 1 v. Omni Vision Techs., Inc.,* 246 F. Supp. 3d 1001, 1003-04 (D. Del. 2017). Defendants' reliance on *MEC Resources, LLC v. Apple, Inc.* is inapposite because the court's finding that considerations of court congestion weighed in favor of transfer was based largely on the prospect of avoiding an allocation of Delaware's judicial resources to resolve a dispute between citizens of California and North Dakota. C.A. No. 17-223-MAK, 2017 WL 4102450, at *5 (D. Del. Sept. 15, 2017). In contrast, Visa is a Delaware corporation. This factor is neutral.

(c) Local interest

The local interest factor is generally neutral in patent litigation because patent cases "implicate[] constitutionally protected property rights, [are] governed by federal law reviewed by a court of appeals of national (as opposed to regional) stature, and affect[] national (if not global) markets." *C.R. Bard, Inc. v. Angiodynamics, Inc.,* 156 F. Supp. 3d 540, 547 (D. Del. 2016) (citing

[4] USR counters with statistics of its own, stating that the Northern District of California has 622 pending actions per judge to 515 per judge in this district, and noting that the average time to trial in civil cases is faster in Delaware than it is in the Northern District of California. (D.I. 35, Ex. B)

Cradle IP v. Texas Instruments, Inc., 923 F. Supp. 2d 696, 700-01 (D. Del. 2013)); *see also Tessera,* 2017 WL 1065865, at *11. Because USR brings only federal patent law claims, the local interest factor is neutral.

4. Transfer analysis summary

As a whole, the *Jumara* factors weigh against transfer. Although USR's forum preference is given slightly less deference because USR does not maintain a place of business in Delaware, it is accorded more weight than defendants' choice of forum. Defendants have shown that most of the relevant evidence and witnesses are located in the Northern District of California, but have not shown that the evidence and witnesses would be unavailable if the case is not transferred. USR has established that it is a small company with limited financial resources in comparison to Apple and Visa, and Delaware is a more convenient forum for it as a party to the action. The remaining factors are neutral. For these reasons, I recommend that the court deny defendants' motion to transfer venue.

B. Patentability Under § 101

1. Legal standard

Defendants move to dismiss the pending action pursuant to Rule 12(b)(6), which permits a party to seek dismissal of a complaint for failure to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). When considering a Rule 12(b)(6) motion to dismiss, the court must accept as true all factual allegations in the complaint and view them in the light most favorable to the plaintiff. *Umland v. Planco Fin. Servs.,* 542 F.3d 59, 64 (3d Cir. 2008). According to defendants, USR's complaint fails to state a claim

because the patents-in-suit are ineligible for patent protection under 35 U.S.C. § 101.

Section 101 provides that patentable subject matter extends to four broad categories, including "new and useful process[es], machine[s], manufacture, or composition[s] of matter." 35 U.S.C. § 101; *see also Bilski v. Kappos,* 561 U.S. 593, 601 (2010) (*"Bilski II"*); *Diamond v. Chakrabarty,* 447 U.S. 303, 308 (1980). The Supreme Court recognizes three exceptions to the statutory subject matter eligibility requirements: "laws of nature, physical phenomena, and abstract ideas." *Bilski II,* 561 U.S. at 601. In this regard, the Supreme Court has held that "[t]he concepts covered by these exceptions are 'part of the storehouse of knowledge of all men . . . free to all men and reserved exclusively to none.'" *Id.* at 602 (quoting *Funk Bros. Seed Co. v. Kalo Inoculant Co.,* 333 U.S. 127, 130 (1948)). At issue in the present case is the third category pertaining to abstract ideas, which "embodies the longstanding rule that an idea of itself is not patentable." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l,* 134 S. Ct. 2347, 2355 (2014) (internal quotations omitted).

In *Mayo Collaborative Services v. Prometheus Laboratories, Inc.,* 566 U.S. 66 (2012), the Supreme Court articulated a two-step "framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice,* 134 S. Ct. at 2355. In accordance with the first step of the *Alice* test, the court must determine whether the claims at issue are directed to a patent-ineligible concept. *See id.* If so, the court must turn to the second step, under which the court must identify 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.* (certain quotation marks omitted). The two steps are "plainly related" and "involve overlapping scrutiny of the content of the claims." *Elec. Power Grp., LLC v. Alstom S.A.,* 830 F.3d 1350, 1353 (Fed. Cir. 2016).

At step 1, "the claims are considered in their entirety to ascertain whether their character as a whole is directed to excluded subject matter." *Internet Patents Corp. v. Active Network, Inc.,* 790 F.3d 1343, 1346 (Fed. Cir. 2015); *see also Affinity Labs of Texas, LLC v. DIRECTV, LLC,* 838 F.3d 1253, 1257 (Fed. Cir. 2016) ("The 'abstract idea' step of the inquiry calls upon us to look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter."). However, "courts must be careful to avoid oversimplifying the claims by looking at them generally and failing to account for the specific requirements of the claims." *McRO, Inc. v. Bandai Namco Games Am. Inc.,* 837 F.3d 1299, 1313 (Fed. Cir. 2016) (internal quotation marks omitted). "Whether at step one or step two of the *Alice* test, in determining the patentability of a method, a court must look to the claims as an ordered combination, without ignoring the requirements of the individual steps." *Enfish,* 822 F.3d at 1338.

At step 2, the Federal Circuit instructs courts to "look to both the claim as a whole and the individual claim elements to determine whether the claims contain 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." *McRO,* 837 F.3d at 1312 (internal brackets and quotation marks omitted). Under the step 2 inquiry, the court must consider whether claim

elements "simply recite 'well-understood, routine, conventional activit[ies].'" *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC,* 827 F.3d 1341, 1350 (Fed. Cir. 2016) (quoting *Alice,* 134 S. Ct. at 2359). "Simply appending conventional steps, specified at a high level of generality, [is] not enough to supply an inventive concept." *Alice,* 134 S. Ct. at 2357 (internal quotation marks omitted).

The Federal Circuit looks to the claims as well as the specification in performing the "inventive concept" inquiry. *See Affinity Labs of Texas v. Amazon.com Inc.,* 838 F.3d 1266, 1271 (Fed. Cir. 2016) ("[N]either the claim nor the specification reveals any concrete way of employing a customized user interface."). "The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art." *Bascom,* 827 F.3d at 1350. In *Bascom,* the Federal Circuit held that "the limitations of the claims, taken individually, recite generic computer, network and Internet components, none of which is inventive by itself," but nonetheless determined that the patent adequately alleged an ordered combination of these limitations to be patent-eligible under step 2 at the pleading stage. *Id.* at 1349.

The "mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention" under step 2. *Alice,* 134 S. Ct. at 2358. "Given the ubiquity of computers . . . wholly generic computer implementation is not generally the sort of additional feature that provides any practical assurance that the process is more than a drafting effort designed to monopolize the abstract idea itself." *Id.* (internal citation and quotation marks omitted). For the second step of the *Alice* framework, the machine-or-transformation test may provide a "useful

clue," although it is not determinative. *Ultramercial, Inc. v. Hulu, LLC,* 772 F.3d 709, 716 (Fed. Cir. 2014) (citing *Bilski II,* 561 U.S. at 604 and *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Canada,* 687 F.3d 1266, 1278 (Fed. Cir. 2012)). A claimed process can be patent-eligible under § 101 consistent with the machine-or-transformation test if it "uses a particular machine or apparatus" and does not "pre-empt[5] uses of the principle that do not also use the specified machine or apparatus in the manner claimed." *In re Bilski,* 545 F.3d 943, 954 (Fed. Cir. 2010), *aff'd sub nom., Bilski v. Kappos,* 561 U.S. 593 (2010).

Patent eligibility under § 101 is a question of law suitable for resolution on a motion to dismiss for failure to state a claim under Rule 12(b)(6). *See In re TLI Commc'ns LLC Patent Litig.,* 823 F.3d 607, 610 (Fed. Cir. 2016) (applying regional circuit law to the de novo review of a district court's patent eligibility determination under § 101 on a Rule 12(b)(6) motion

---

[5] At both steps 1 and 2 of the *Alice* inquiry, the Federal Circuit considers the issue of preemption to determine whether a patent is not directed to a specific invention and instead would monopolize "the basic tools of scientific and technological work," thereby "imped[ing] innovation more than it would tend to promote it" and "thwarting the primary object of the patent laws." *Alice,* 134 S. Ct. at 2354; *see also McRO,* 837 F.3d at 1315 (applying the doctrine of preemption and concluding that a claim was patent-eligible at step 1); *Bascom,* 827 F.3d at 1350 (applying the doctrine of preemption and concluding that a claim was patent-eligible at step 2). "[T]he focus of preemption goes hand-in-hand with the inventive concept requirement." *Jedi Techs., Inc. v. Spark Networks, Inc.,* C.A. No. 16-1055-GMS, 2017 WL 3315279, at *8 n.2 (D. Del. Aug. 3, 2017) (quoting *Tenon & Groove, LLC v. Plusgrade S. E. C.* , C.A. No. 12-1118-GMS, 2015 WL 1133213, at *4 (D. Del. Mar. 11, 2015)). However, "the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.,* 788 F.3d 1371, 1379 (Fed. Cir. 2015).

to dismiss). However, the Federal Circuit recently emphasized that, "like many legal questions, there can be subsidiary fact questions which must be resolved en route to the ultimate legal determination." *Aatrix Software, Inc. v. Green Shades Software, Inc.,* 882 F.3d 1121, 1128 (Fed. Cir. 2018). "The 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[]" that goes beyond what was simply known in the prior art. *Berkheimer v. HP Inc.,* 881 F.3d 1360, 1368 (Fed. Cir. 2018). On a motion to dismiss, this question of fact, like all questions of fact, must be resolved in the plaintiff's favor. *Aatrix Software, Inc.,* 882 F.3d at 1128.

2. Analysis

As a preliminary matter, the court addresses the parties' disagreement as to whether the claims addressed in the briefs are adequately representative of the remaining 107 asserted claims across the four patents-in-suit. Defendants address one claim from each patent-in-suit described by USR as "exemplary" in the complaint. (D.I. 1 at ¶¶ 43, 65, 84, 106) Defendants contend that USR's use of the word "exemplary" and the fact that "all of the claims effectively cover the same core system with some variations[]" indicate that the chosen claims are representative. (12/13/17 Tr. 15:4-8) USR charges defendants with failing to meet their burden to establish how the four claims are representative of the 107 asserted claims which are not discussed, drawing a semantic distinction between "exemplary" and "representative." (D.I. 30 at 20)

While defendants bear the burden of proof to establish the exemplary nature of an asserted claim, USR's representations in the complaint itself support defendants' position that the identified claims are

sufficiently representative. At oral argument, USR denied that the claims relied upon by defendants are representative of the remaining 107 claims, but offered no support for its position. (12/13/17 Tr. 56:20-23, 57:6-8) ("Those representations and allegations in our complaint are not meant to take the place of detailed infringement allegations and we submit they do not . . . . Do we think [the example in the complaint is] representative of infringement for every claim of every asserted patent? Absolutely not."). Having considered the parties' positions and the facts before the court, I recommend that the court treat the claims addressed in the briefing as adequately representative of the remaining 107 asserted claims across the patents-in-suit for purposes of the pending motion.

(a) '539 patent

(i) *Alice* Step 1

Applying the first step of the *Alice* framework to the asserted claims, the court concludes that exemplary claim 22 of the '539 patent is not directed to an abstract idea because "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Visual Memory LLC v. NVIDIA Corp.,* 867 F.3d 1253, 1258 (Fed. Cir. 2017) (quoting *Enfish,* 822 F.3d at 1336). The preamble of claim 22 recites "[a] method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code." ('539 patent, col. 20:4-7) Claim 22 subsequently lists the following requirements: (1) receiving a transaction request including a time-varying multicharacter code; (2) mapping the time-varying multicharacter code to the identity of

the user; (3) determining compliance with access restrictions to secure data; (4) accessing information of the entity required to perform the transaction based on access restrictions; (5) providing the account identifying information to a third party without providing such information to the provider to enable or deny the transaction; and (6) enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information. (*Id.,* col. 20:9-31)

Verifying account information to enable a transaction is a well-known practice, as "determination/verification of a person's identity will typically dictate extension of credit, granting access to information, allowing entry to a restricted area, or the granting of numerous other privileges." ('539 patent, col. 1:46-52) However, the '539 patent is directed to an improvement in computer functionality by enabling anonymous identification, which secures the transaction without giving the merchant identifying information such as a credit card number. ('539 patent, col. 2:17-22, 2:64-3:1) The time-varying multicharacter code claimed in the '539 patent obviates the need for encryption of the identifying data, (*id.,* col. 13:43-51), and the anonymous identification system protects the credit card information from theft or fraud by the merchant, (*id.,* col. 2:17-22; 12:11-18). The '539 patent specification confirms that "conventional identification devices require that at least some personal information be transmitted to complete a transaction." (*Id.,* col. 2:24-27) Consequently, the claims of the '539 patent represent a technological improvement sufficient to distinguish the invention from an unpatentable abstract idea. *See Visual Memory,* 867 F.3d at 1259.

(ii) *Alice* Step Two

Having determined that claim 22 of the '539 patent is not directed to an abstract idea, the court need not proceed to the second step of the *Alice* test to determine whether the patent describes an inventive concept.[6] As previously stated, the '539 patent claims the inventive concept of enabling anonymous identification to secure a transaction without giving the merchant identifying information such as a credit card number. ('539 patent, col. 2:17-22, 2:64-3:1); *see also Elec. Power Grp., LLC v. Alstom SA.,* 830 F.3d 1350, 1353 (Fed. Cir. 2016) (acknowledging significant overlap between step 1 and step 2 of the *Alice* inquiry).

(b) '826 patent

(i) *Alice* Step 1

Applying the first step of the *Alice* framework, the court concludes that exemplary claim 10 of the '826 patent is not directed to an abstract idea because "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Visual Memory LLC v. NVIDIA Corp.,* 867 F.3d 1253, 1258 (Fed. Cir. 2017) (quoting *Enfish,* 822 F.3d at 1336). The preamble of claim 10 recites "[a] computer implemented method of authenticating an identity of a first entity." ('826 patent, col. 45:30-31) Claim 10 subsequently identifies the following re-

---

[6] The court has considered the recent supplemental authority from the Federal Circuit which was submitted by USR at D.I. 49 and D.I. 50. However, the Federal Circuit's decisions in both *Aatrix* and *Berkheimer* focused on the district court's analysis under the second step of the *Alice* inquiry, which the court does not reach in the present analysis. *See Aatrix,* 882 F.3d at 1128; *Berkheimer,* 881 F.3d at 1367-68.

quirements: (1) authenticating the user of a first handheld device; (2) retrieving or receiving the user's biometric information; (3) determining a first authentication information from the first biometric information; (4) receiving with a second device the first authentication information; (5) retrieving or receiving second authentication information for the user; and (6) authenticating the identity of the user based on both the first and second authentication information. (*Id.,* col. 45:32-47) Like the '539 patent, the '826 patent provides a more secure authentication system. The '826 patent adds requirements pertaining to biometric information and implementation on a handheld mobile device, representing a technological improvement as opposed to an abstract idea.

Although limiting the claimed method to handheld devices is not sufficient, by itself, to avoid categorization as an abstract idea, *Alice* requires the court to consider the claim's elements "both individually and as an ordered combination" to determine whether the nature of the claim is transformed into a patent-eligible application. *Alice,* 134 S. Ct. at 2350; *see also Bascom,* 827 F.3d at 1349 (concluding that claims contained an inventive concept even though the limitations recited generic, non-inventive computer, network, and Internet components). The '826 patent is directed to an improvement in computer functionality, as it requires biometric information to locally authenticate the user as well as a second level of remote user authentication. ('826 patent, col. 32:43-56; col. 34:7-25) While certain elements of claim 10 recite generic steps of authenticating a user based on biometric information, the claim as a whole describes an improved distributed authentication system with increased security. Thus, the facts presently before the court are distinguishable from those before the Northern

District of Illinois in *IQS US Inc. v. Calsoft Labs Inc.,* because the '826 patent presents "an unconventional technological solution . . . to a technological problem." 2017 WL 3581162, at *5 (N.D. Ill. Aug. 18, 2017) (quoting *Amdocs* (*Israel*) *Ltd. v. Openet Telecom, Inc.,* 841 F.3d 1288 (Fed. Cir. 2016)).

(ii) *Alice* Step Two

Having determined that claim 10 of the '826 patent is not directed to an abstract idea, the court need not proceed to the second step of the *Alice* test to determine whether the patent describes an inventive concept. As previously stated, the '826 patent claims the inventive concept of a more secure mobile authentication system to resolve security issues specific to remote authentication. *See Elec. Power Grp., LLC v. Alstom S.A.,* 830 F.3d 1350, 1353 (Fed. Cir. 2016) (acknowledging significant overlap between step 1 and step 2 of the *Alice* inquiry).

(c) '137 patent

(i) *Alice* Step 1

Applying the first step of the *Alice* framework to the asserted claims, the court concludes that exemplary claim 12 of the '137 patent is not directed to an abstract idea because "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Visual Memory LLC v. NVIDIA Corp.,* 867 F.3d 1253, 1258 (Fed. Cir. 2017) (quoting *Enfish,* 822 F.3d at 1336). The preamble of claim 12 recites "[a] system for authenticating a user for enabling a transaction." ('137 patent, col. 46:55-56) Claim 12 subsequently lists the elements of a system comprising: (1) a first device with a biometric sensor; (2) a first processor programmed to authenticate the

user of the first device, retrieve or receive the user's biometric information, authenticate the user of the first device based on the biometric, and generate a signal; (3) a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the signals to a second device; and (4) the first processor is programmed to receive an enablement signal indicating an approved transaction from the second device based on acceptance of the biometric authentication as well as the first and second authentication information to enable the transaction. (*Id.,* col. 46:57-47:14) The claimed system generates a time variant or other type of code which can only be used for a single transaction, preventing the merchant from retaining information that could be fraudulently used in subsequent transactions. (*Id.,* col. 18:14-34) The '137 patent thus provides a more secure mobile transaction authentication system with both local and remote authentication, addressing a problem specific to the security of mobile devices.

Although limiting the claimed system to mobile device transactions is not sufficient, by itself, to avoid categorization as an abstract idea, *Alice* requires the court to consider the claim's elements "both individually and as an ordered combination" to determine whether the nature of the claim is transformed into a patent-eligible application. *Alice,* 134 S. Ct. at 2350; *see also Bascom,* 827 F.3d at 1349 (concluding that claims contained an inventive concept even though the limitations recited generic, non-inventive computer, network, and Internet components). The '137 patent is directed to an improvement in the security of mobile devices by using biometric information to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be

fraudulently used in subsequent transactions. ('137 patent, col. 18:14-34) While certain elements of claim 12 recite generic computer components, the claim as a whole describes an improved authentication system with increased security. The facts presently before the court are distinguishable from those before the court in *Walker Digital, LLC v. Google, Inc.,* because the '137 patent is not a computerization of a preexisting transaction approval process, but instead teaches the use of a predetermined algorithm at both the user's device and at the USR. 66 F. Supp. 3d 501, 511 (D. Del. 2014).

(ii) *Alice* Step Two

Having determined that claim 12 of the '137 patent is not directed to an abstract idea, the court need not proceed to the second step of the *Alice* test to determine whether the patent describes an inventive concept. As previously stated, the '137 patent claims the inventive concept of a more secure mobile authentication system to resolve security issues specific to remote authentication. *See Elec. Power Grp., LLC v. Alstom S.A.,* 830 F.3d 1350, 1353 (Fed. Cir. 2016) (acknowledging significant overlap between step 1 and step 2 of the *Alice* inquiry).

(d) '813 patent

(i) *Alice* Step 1

Applying the first step of the *Alice* framework to the asserted claims, the court concludes that exemplary claim I of the '813 patent is not directed to an abstract idea because "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Visual Memory LLC v. NVIDIA Corp.,* 867 F.3d 1253, 1258 (Fed. Cir. 2017)

(quoting *Enfish,* 822 F.3d at 1336). The preamble of claim 1 recites "[amn electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction." ('813 patent, col. 51:65-67) Claim 1 subsequently lists the elements of the device comprising: (1) a biometric sensor; (2) a user interface; (3) a communication interface; and (4) a processor coupled to the biometric sensor. (*Id.,* col. 52:1-23) The claimed invention describes several means of authenticating user information to prevent unauthorized use of the electronic ID device. (*Id.,* col. 45:55-46:67; 50:1-22; 51:7-26) The '813 patent thus provides a series of claim dements operating together in a specific way to provide a more secure mobile transaction authentication system with both local and remote authentication, addressing a problem specific to the security of mobile devices without covering, and preempting, every "way[ ] you can authenticate a mobile device payment transaction[.]" (12/13/17 Tr. 39:8-14); *see McRO, Inc. v. Bandai Namco Games Am. Inc.,* 837 F.3d 1299, 1313 (Fed. Cir. 2016) ("Whether at step one or step two of the *Alice* test . . . a court must look to the claims as an ordered combination, without ignoring the requirements of the individual steps. The specific, claimed features of these rules allow for the improvement realized by the invention.").

Although limiting the claimed system to verifying an account holder's identity with code and identifying information before enabling a transaction is not sufficient, by itself, to avoid categorization as an abstract idea, *Alice* requires the court to consider the claim's elements "both individually and as an ordered combination" to determine whether the nature of the claim is transformed into a patent-eligible application. *Alice,* 134 S. Ct. at 2350; *see also Bascom,* 827 F.3d at 1349

(concluding that claims contained an inventive concept even though the limitations recited generic, non-inventive computer, network, and Internet components). The '813 patent is directed to an improvement in the security of mobile devices by using a biometric sensor, a user interface, a communication interface, and a processor working together to generate a time varying or other type of code that can be used for a single transaction, preventing the merchant from retaining identifying information that could be fraudulently used in subsequent transactions. ('813 patent, col. 52:1-29) While certain elements of claim 1 recite generic computer components, the claim as a whole describes an improved authentication system with increased security. The facts presently before the court are distinguishable from those before the Federal Circuit in *Digitech Image Technologies, LLC v. Electronics for Imaging, Inc.,* because the '813 patent claims are tied to a tangible device with a biometric sensor, user interface, processor, and other elements. 758 F.3d 1344, 1350 (Fed. Cir. 2014).

The present case is also distinguishable from the Federal Circuit's recent decisions in *Secured Mail Solutions LLC* and *Smart Systems Innovations, LLC,* which defendants raised at oral argument. (12/13/17 Tr. 43:2-21) The '813 patent claims a series of specific elements operating together in a specific way to provide a tangible device that provides a more secure authentication system. In contrast, the patent claims in *Secured Mail Solutions LLC v. Universal Wilde, Inc.,* which provided a method for generation and mailing of a barcode, were "not limited to any particular technology of generating, printing, or scanning a barcode, of sending a mail object, or of sending the recipient-specific information over a network. Rather, each step of the process is directed to the abstract

process of communicating information about a mail object using a personalized marking." 873 F.3d 905, 911 (Fed. Cir. 2017). Similarly, in *Smart Systems Innovations, LLC v. Chicago Transit Authority,* the Federal Circuit concluded that the asserted claims were not "directed to specific rules that improve a technological process, but rather invoke computers in the collection and arrangement of data." 873 F.3d 1364, 1372-73 (Fed. Cir. 2017). Claim 1 of the '813 patent is distinguishable from these abstract ideas because the claimed electronic ID device is limited to a particular technology comprising a biometric sensor, a user interface, a communication interface, and a processor, each of which is narrowly configured to the claimed invention as an improvement to the technology. ('813 patent, col. 51:65-52:29)

According to defendants, four pending patent applications that are continuations of the '813 patent also support their position that the patents-in-suit are invalid under 35 U.S.C. § 101. (D.I. 44 at 1) At oral argument, defendants argued that the non-final rejection of U.S. Application No. 14/071,126 ("the '126 application") for patent ineligibility is significant because its claims have substantial similarities to the claims of the '813 patent. (12/13/17 Tr. 6:9-16) However, consistent with the representations made by the court during the oral argument, the court does not consider the non-final rejection of the '126 application to be "outcome determinative." (12/13/17 Tr. at 8:13-19)

(ii) *Alice* Step Two

Having determined that claim 1 of the '813 patent is not directed to an abstract idea, the court need not proceed to the second step of the *Alice* test to determine whether the patent describes an inventive concept. As previously stated, the '813 patent claims

the inventive concept of a more secure mobile authentication system to resolve security issues specific to remote authentication. *See Elec. Power Grp., LLC v. Alstom S.A.,* 830 F.3d 1350, 1353 (Fed. Cir. 2016) (acknowledging significant overlap between step 1 and step 2 of the *Alice* inquiry).

IV. CONCLUSION

For the foregoing reasons, I recommend that the court deny defendants' motion to transfer (D.I. 21), and deny defendants' motion to dismiss pursuant to Rule 12(b)(6) (D.I. 16).

This Report and Recommendation is filed pursuant to 28 U.S.C. § 636(b)(1)(B), Fed. R. Civ. P. 72(b)(1), and D. Del. LR 72.1. The parties may serve and file specific written objections within fourteen (14) days after being served with a copy of this Report and Recommendation. Fed. R. Civ. P. 72(b)(2). The objections and responses to the objections are limited to ten (10) pages each. The failure of a party to object to legal conclusions may result in the loss of the right to de novo review in the District Court. *See Sincavage v. Barnhart,* 171 F. App'x 924, 925 n.1 (3d Cir. 2006); *Henderson v. Carlson,* 812 F.2d 874, 878-79 (3d Cir. 1987).

The parties are directed to the court's Standing Order For Objections Filed Under Fed. R. Civ. P. 72, dated October 9, 2013, a copy of which is available on the court's website, http://www.ded.uscourts.gov.

Dated: September 19, 2018

/s/ Sherry R. Fallon
Sherry R. Fallon
UNITED STATES MAGISTRATE JUDGE

APPENDIX D

NOTE: This order is nonprecedential.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

[Filed October 29, 2021]

2020-2044

UNIVERSAL SECURE REGISTRY LLC,
Plaintiff-Appellant,

v.

APPLE INC., VISA INC., VISA U.S.A. INC.,
Defendants-Appellees.

Appeal from the United States District Court for the District of Delaware in No. 1:17-cv-00585-CFC-SRF, Judge Colm F. Connolly.

ON PETITION FOR PANEL REHEARING
AND REHEARING EN BANC

Before NEWMAN, LOURIE, DYK, PROST, REYNA, WALLACH[*], TARANTO, CHEN, HUGHES, STOLL, and CUNNINGHAM, *Circuit Judges*.[**]

---

[*] Circuit Judge Wallach participated only in the decision on the petition for panel rehearing.

[**] Chief Judge Moore and Circuit Judge O'Malley did not participate.

PER CURIAM.

ORDER

Universal Secure Registry LLC filed a combined petition for panel rehearing and rehearing en banc. The petition was referred to the panel that heard the appeal, and thereafter the petition for rehearing en banc was referred to the circuit judges who are in regular active service.

Upon consideration thereof,

IT IS ORDERED THAT:

The petition for panel rehearing is denied.

The petition for rehearing en banc is denied.

The mandate of the court will issue on November 5, 2021.

October 29, 2021
Date

FOR THE COURT

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court