IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

UNIVERSAL SECURE REGISTRY LLC, *Plaintiff*, v. APPLE INC., VISA INC., and VISA U.S.A., INC., *Defendants*.	Civ. No. 17-585-CFC-SRF

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.*

MEMORANDUM OPINION

June 30, 2020
Wilmington, Delaware

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]

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

[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.

"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 send[ing] 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 authenticating 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.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

UNIVERSAL SECURE REGISTRY LLC, *Plaintiff*, v. APPLE INC., VISA INC., and VISA U.S.A., INC., *Defendants*.	Civ. No. 17-585-CFC-SRF

ORDER

IT IS HEREBY ORDERED, for the reasons stated in the accompanying Memorandum Opinion, that:

1. The Magistrate Judge's recommendation that the Court deny Defendants' motion to dismiss (D.I. 137) is REJECTED and Defendants' objections to that recommendation (D.I. 147) are SUSTAINED;

2. Defendants' motion to dismiss (D.I. 16) is GRANTED;

3. The Complaint (D.I. 1) is DISMISSED WITH PREJUDICE; and

4. The Clerk of the Court is directed to close the case.

Dated: June 30, 2020

UNITED STATES DISTRICT JUDGE