IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| UNIVERSAL SECURE REGISTRY LLC,<br><br>*Plaintiff*,<br><br>v.<br><br>APPLE INC., VISA INC., and VISA U.S.A., INC.,<br><br>*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

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.