UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

UNIFIED PATENTS INC.
Petitioner

v.

UNIVERSAL SECURE REGISTRY, LLC
Patent Owner

_____

IPR2018-00067
Patent 8,577,813

_____

DECLARATION OF DR. ERIC COLE IN SUPPORT OF PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

I, Eric Cole, hereby declare the following:

I. BACKGROUND AND QUALIFICATIONS

1. I have been asked to respond to certain opinions provided by Dr. Markus Jacobsson in his declaration (EX2004) that accompanied Patent Owner's Response and that responded to my original declaration (EX1009) in this matter..

2. My opinions in my original declaration remain the same. Additionally, as before, I offer the below opinions and background knowledge from the lens of a person having ordinary skill in the art at the time of the earliest possible priority date of the '813 Patent, which I have been told to assume is February 21, 2006 (a "PHOSITA").[1]

3. As part of my work in connection with this declaration, I have reviewed the following materials in addition to those materials already reviewed in preparation of my original declaration (EX1009) and those materials reviewed in preparation of my recent declaration in support of Petitioner's Response to Patent Owner's Contingent Motion to amend (EX1022):

[1] This February 21, 2006 is the same earliest possible priority date I was instructed to assume in my original declaration. *See* EX1009, at ¶26. I note that I had a typographical error in my Declaration in Support of Petitioner's Opposition to Patent Owner's Contingent Motion to Amend, which had stated an assumed date of "June 9, 2006." EX1022, at ¶2. In preparing that declaration, I had applied the same assumed priority date set forth in my original declaration (i.e., February 21, 2006). In any event, my opinions would not have changed based on that slight difference in assumed priority dates.

- PO's Preliminary Response (Paper 7);
- Declaration of Dr. Jakobsson (EX1033);
- U.S. Pub. 2003/0093690 to Kemper ("*Kemper*") (EX1034);
- U.S. Pub. 2004/0111343 to Lindvall ("*Lindvall*") (EX1035).

II. OPINION

A. Additional Background of Technology

Multi-factor Authentication

4. As I mentioned in both of my previous declarations, it was well known in the art by 2006 that systems requiring multi-factor authentication (e.g., the use of a PIN and a biometric verification) provided enhanced security against theft compared to systems requiring only one source of information for authentication. Dr. Jakobsson appears to opine the opposite, namely, that it would not "enhance security" to employ a system requiring both types of authentication. *See, e.g.*, *Jakobsson Decl.* (EX2004) at ¶92. Respectfully, I disagree—systems using multi-factor authorization techniques were (and are) almost universally more secure than systems using only one factor. But a PHOSITA in 2006 was highly motivated to incorporate different types of authentication into financial transactions, both to prevent unscrupulous third parties from accessing or using the user's financial data and to confirm to a verifier that a financial service is being requested by an authorized user. Systems requiring multiple types of authentication presented more obstacles to a would-be attacker because the compromise of the

first source (e.g., a PIN being overheard or seen, or a system being hacked for biometric information) would not necessarily implicate the second.

5. For example, *Jin et al*., cited in my original declaration, provide some reasons that were known to a PHOSITA as to why systems using both biometrics and secret information to authenticate a user was more desirable than the use of biometrics alone or secret information, such as a PIN, alone. PINs suffered from the weakness that they could be illicitly acquired through observation by an unscrupulous party, while a person's biometrics suffer from a different weakness in that, if compromised, they cannot be changed and place a user at risk for an attacker masquerading as them.[2]

6. A PHOSITA would have recognized that requiring both types of information for verification of a user would allow each source to reconcile the deficiencies of the other. For example, it wouldn't matter if the PIN were illicitly observed, because an unscrupulous observer could not "know" the user's biometrics. Additionally, even if biometrics were somehow mimicked, an attacker could not mimic a PIN—it is either known, or it isn't. Therefore, it was commonly

[2] *See Jin* (EX1012) at 1-2, 10 (Note: To provide ease of reference, I refer to the exhibit page number for non-patent or patent publication references); *see also Cole Decl.* (EX1009) at ¶34.

accepted that "wider adoption of two-factor authentication is desirable" in e-commerce by 2006.[3]

Multi-Layered Authentication

7. Multi-layered authentication (i.e., authentication at multiple places in a security system) was also well-known in the art and had cognizable benefits. For example, U.S. Pub. 2003/0093690 to *Kemper* (issued as U.S. Pat. 7,222,361), entitled "Computer Security With Local And Remote Authentication," describes a system in which a user must first be authenticated at a local database to access services, and then and a remote database in the same session to continue services.[4]

8. A PHOSITA would have particularly recognized the pros of such an arrangement in the context of multi-purpose identification devices, such as PDAs or cell phones. A user may wish to access such devices for reasons other than a financial transaction, such as to call or send a message to a friend, look at a photo stored on the device, or change settings on the device. Local authentication using, for example, secret information and/or a biometric input, protects this information from unwanted intruders, who may be people with as simple means as your

[3] *See Harris* (EX1013) at 1:28-64; *see also Kemper* (EX1034) at [0002] ("'[S]trong authentication" uses a combination of items belonging to at least two of the following three categories: 1) personal knowledge (such as a password or personal identification number); 2) personal possessions (such a cardkey or other physical token); and 3) personal characteristics (such as a handwriting sample, voiceprint, fingerprint, or retina scan).")

[4] *Kemper* (EX1034) at Abstract, [0027]-[0029] Figs. 3-4

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.