

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

Case No. IPR2024-01333
U.S. Patent No. 8,352,730

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Relief Requested.....	1
II.	The '730 Patent.....	1
	A. Overview	1
III.	Claim Construction.....	4
IV.	Level of Ordinary Skill.....	5
V.	Ground 1: Claims 1, 2, 4-6, 8, 9, 11, 12, and 14-17 Are Obvious Over Ludtke.	5
	A. Overview of Prior Art Ludtke	5
	B. Claims.....	9
	1. Independent claim 1	9
	a. [1preamble]: “A method for verifying a user during authentication of an integrated device, comprising the steps of:”	9
	b. [1ai]: “persistently storing biometric data of the user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]”	11
	c. [1aii]: “[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered]”	14
	d. [1aiii]: “[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;”	16

- e. [1b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;”23
 - f. [1c]: “responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;”23
 - g. [1d]: “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;”25
 - h. [1e]: “responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and”25
 - i. [1f]: “responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.”32
- 2. Claim 2: “The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.”36
 - 3. Claim 4: “The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.”36

4.	Claim 5: “The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.”	38
5.	Claim 6: “The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication”	38
6.	Independent Claim 8	39
a.	[8preamble]: “An integrated device for verifying a user during authentication of the integrated device, comprising:”	39
b.	[8ai]: “a memory stores biometric data of a user, and”	39
c.	[8aii]: “a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and”	39
d.	[8aiii]: “a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;”	39
e.	[8b]: “wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;”	39
f.	[8c]: “a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein	

the one or more codes and the other data values includes the device ID code; and”40

g. [8d]: “responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.”41

7. Claim 9: “The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.”42

8. Claim 11: “The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.”42

9. Independent Claim 1245

a. [12preamble]: “A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:”45

b. [12a]: “receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices”47

c. [12b]: “requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the

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.