UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY AB, ASSA ABLOY INC.,
HID Global Corporation, ASSA ABLOY Global Solutions, Inc.,
and Master Lock Company, LLC
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY LTD.,
Patent Owner.

Case IPR2022-01045
Patent 9,269,208

PATENT OWNER'S RESPONSE TO PETITIONER'S SUPPLEMENTAL BRIEF AFTER REMAND

The Board's inclusion of "provides secure access to a controlled item" as part of the construction of "biometric signal" was appropriate. "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." Paper 42 at p. 70, quoting *Renishaw PLC v Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998). Here, the Board properly concluded that "provides secure access to a controlled item" was appropriate because it stays true to the claim language and most naturally aligns with the '208 Patent's description of the invention. *Id*. at 70. Under the Board's construction none of Petitioner's prior art discloses elements 1[D(1)-D(3)][1] of the '208 Patent. Nor is any aspect of the Board's FWD inconsistent with the Apple Final Written Decision ("Apple FWD").

I. Inclusion of "Provides Secure Access" Is Proper

A. The Board's Analysis Was Sound

The Board's inclusion of "provides secure access" was proper.[2] As noted in the FWD, the express objective of the claimed invention is a "system for providing

[1] This claim element numbering was used in the briefing and in the FWD. *See e.g.,* Paper 42 at p. 82.

[2] Patent Owner argued that "biometric signal" should be limited to a physical attribute of a user. The Board disagreed and concluded that "biometric signal" includes both physical and behavioral attributes. Patent Owner maintains, for the reasons stated in Patent Owner's Response and Sur-Reply, that the construction of "biometric signal" should be limited to physical attributes of the user. *See e.g.*, Paper 26, pp. 8-15; Paper 36, pp. 7-9.

secure access to a controlled item." Paper 42, p. 62; *see also* Ex. 1007, *e.g.,* Claims 1, 2, 6, 9, 10. The specification is replete with discussion of the invention being designed to provide "secure access." *See e.g.*, Ex. 1007, Abstract, 1:14-16, 2:26-28, 2:35-39, 2:44-53, 2:57-65, 5:51-52, 7:16-20, 11:47-53, 14:11-35.[3] For the claimed system to achieve this object, it is the "biometric signal" that must be an input capable of providing secure access; it must uniquely identify the user. The first step in the claimed enrollment is the entry of the biometric signal. Ex. 1007, Figs 6 and 8 and 12:39-54.[4] If the biometric signal did not uniquely identify the user then it could not grant secure access, as Petitioner's expert agreed. *See* Ex. 2040, 17[5]:12-15 ("When a biometric system is used for the purpose of providing access, then it would need to be capable of uniquely identifying the user."); Ex. 1029, ¶ 14 ("So long as the biometric sensor can output a biometric signal capable of uniquely identifying a user, the claims and reported invention would be viable."). This point is further recognized in the definition of a "fingerprint" cited the Board ("the pattern of curved lines on the end of a finger *that is different in every person*…", Paper 42, p. 64) (emphasis added), and also in Petitioner's cited prior art. *See* Ex. 1004, 3:14-24 (defining biometrics as the "mathematical

[3] The '208 Patent specification uses the phrase "secure access" 73 times.

[4] As in the FWD, citations to the '208 Patent are in Column;Line format.

[5] This is the exhibit page number of the Lipoff transcript, not the deposition page number.

description of characteristic elements of the owner's body…*which describe him uniquely*") (emphasis added); Ex. 1003, Abstract ("Biometric devices…identify a user based on compared measurements of *unique personal characteristics*.") (emphasis added); *see also* Paper 36, pp. 8-9.

The Board correctly noted that the claims require that the "biometric signal" must be able to be "matched to a database." Paper 42, p. 64. "Matching" is required for granting secure access. It is the user's unique biometric signal that allows the system to "match" (or not) and therefore determine secure access. A POSITA would readily understand that it is the ability of the *biometric signal* to distinguish the user that is needed to accomplish the claimed invention's object of granting secure access. Thus, inclusion of "provides secure access to a controlled item" as part of the construction of "biometric signal" is reasonable.

B. Petitioner's Remand Arguments Are Not Persuasive

Petitioner first argues that inclusion of "secure access" is wrong because other components besides the biometric signal also play a role in providing secure access. Paper 54, pp. 2-3. But this argument ignores that it is the biometric signal, not the other components, that includes the unique information that allows the grant of secure access. Ex. 2040, 17:12-15; Ex. 2029, ¶ 14. Enrollment and verification each begin with the input of a biometric signal that a POSITA would understand must be capable of granting secure access. *See e.g.*, Ex. 1007, Figs 6, 7, and 8.

Nor does inclusion of "secure access" in the construction read the "secure access signal" element out of the claims. Paper 54, p. 3. Again, it is the biometric signal that contains the unique information that permits secure access. Ex. 2040, 17:12-15; Ex. 2029, ¶ 14; *see also* Ex. 1007, 8:6-10 ("The step 202 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user…"). Construing the biometric signal to be an attribute that provides secure access does not render meaningless the other claimed components; each still plays its role. Rather, including "secure access" in the "biometric signal" construction appropriately recognizes that a biometric signal is not merely *any* input to the system, but instead is an attribute of the user that can provide secure access. Particularly in the context of the specification's repeated references to the goal of "secure access," a POSITA would interpret "biometric signal" as an input that must be capable of providing secure access.

Second, Petitioner's contention that inclusion of "secure access" "narrows the claims by ignoring the role the biometric signal plays in enrolling new users" (Paper 54, p. 4) misses the mark. The Board's construction in no way precludes the biometric signal from also playing an administrative role; it simply requires

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.