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
Petitioners,

v.

CPC Patent Technologies PTY LTD.,
Patent Owner.

Case No. IPR2022-01089
U.S. Patent No. 9,269,208

PETITIONERS' SUPPLEMENTAL BRIEFING AFTER REMAND

In the Final Written Decision, the Board construed "biometric signal" to mean "physical or behavioral attribute that *provides secure access to a controlled item*." Paper 42 at 61-71 (emphasis added). But a "biometric signal" is not limited to one that "provides secure access." The claims expressly state a separate "secure access signal" is created and sent to a receiver sub-system, so that the receiver sub-system can provide secure access. '208 patent at 15:41-16:3; Ex. 2034, 60:2-10. And the claims and specification establish the biometric signal provides more than just secure access, playing an important administrative role in enrolling users. '208 patent at 10:16-19, 10:45-63, 11:27-29, 15:41-16:3. To capture the full scope of how "biometric signal" is used in the claims and specification, a "biometric signal" should be construed to mean "the input and output of a biometric sensor." Paper 30 (Reply) at 7-11; Ex. 1029 ¶¶ 5-15.

Even if "biometric signal" were limited to one that "provides secure access," however, the prior art discloses it, and the Board's contrary findings contradict the Apple Final Written Decision ("Apple FWD"). There, the Board expressly found that a fingerprint sensor always acts as a fingerprint sensor, even when receiving a succession of finger presses, detecting the biometric part of the input signal, while also sensing the number and duration of inputs. *Apple*, IPR2022-00602, Paper 31 at 31. The prior art here (*Mathiassen-067* and *Bianco*) also uses a biometric sensor to detect a biometric part of an input signal and sense a number and duration of those

inputs. Ex. 1004, 8:25-38. The prior art thus renders obvious the claims under both the proper and contested constructions.

I. A "Biometric Signal" Is Not Required to "Provide[] Secure Access"

The Board construed "biometric signal" to mean a "physical or behavioral attribute that provides secure access to a controlled item." Paper 42 at 61-71. There is no basis for limiting a biometric signal to something that provides secure access. Properly construed, biometric signal is an "input and output of a biometric sensor." Paper 30 (Reply) at 7-11; Ex. 1029 ¶¶ 5-15; Paper 42 at 64 ("'biometric signal' is a signal that can be received by a biometric sensor and . . . matched to a database").

A. The Claim Language Does Not Limit a Biometric Signal to One that "Provides Secure Access"

In the Final Written Decision, the Board noted: "the challenged claims state the specific objective of the claimed invention," namely, "providing secure access to a controlled item." Paper 42 at 62. The Board then imputed that objective to the claimed "biometric signal" specifically, and reasoned: "[t]hus, the purpose of the biometric signal is to achieve this objective—'secure access to a controlled item.'" *Id.*at 62-63. There is no dispute that the claimed biometric signal is *one component* in a larger system that "provides secure access." '208 patent at 15:41-16:3. The claims, however, explain (i) other claim elements provide the secure access, and (ii) although the biometric signal contributes to providing secure access, it *also* has an important role in enrolling users. The Board's construction ignores both points.

Indeed, the '208 claims provide a "system for providing secure access to a controlled item" comprising a transmitter sub-system and receiver sub-system. *Id.* To authenticate and provide secure access, the claims explain that the transmitter sub-system receives "a biometric signal" (at the biometric sensor), compares that signal to a "biometric signatures" database, and transmits a "secure access signal" conveying "an accessibility attribute." *Id.* Then, the receiver sub-system receives that "secure access signal" and provides access to the controlled item based on the "accessibility attribute." *Id.* While the biometric signal *plays a part* in this cascade of steps authenticating and providing secure access, the claims expressly state that an *entirely separate* "secure access signal" is created and sent to the receiver sub-system, so that the receiver sub-system can provide secure access. *Id*; *see also, e.g.*, Ex. 2034, 60:2-10. If it were the biometric signal alone that provided secure access, there would be no need for the later-claimed "secure access signal." The Board's construction effectively reads "secure access signal" out of the claims, and such a construction is disfavored. *See, e.g.*, *Mformation Techs., Inc. v. Rsch. in Motion Ltd.*, 764 F.3d 1392, 1399 (Fed. Cir. 2014).

Moreover, the claims *also separately recite* an administrative and enrollment function, and they explain that the biometric signal plays an important role in this function as well. '208 patent at 15:41-16:3. For example, the claims require the transmitter sub-system to receive "a series of entries of the biometric signal," and

to use a number and duration of those entries to "map[] said series into an instruction" to populate the database of biometric signals. *Id.* at 15:58-67. This is all to enroll a user. *Id.*; *see also* Paper 42 at 63 ("'series of entries of the biometric signal,' for example, to enroll new users, is the Morse-code like entries of 'dit, dit, dit, dah'"); Ex. 2040, 51:21-25. The Board's construction narrows the claims by ignoring the role the biometric signal plays in enrolling new users, *separate from* "provid[ing] secure access." The proper construction would not focus on any one function.

B. The Board's Construction Ignores Disclosed Embodiments

The '208 specification echoes the claim language and shows the claimed "biometric signal" does more than just "provide[] secure access." A "biometric signal" can aid in authentication and secure access. *See* '208 patent at 8:6-17. But the specification also explains that a biometric signal can be used to "take other action," like providing "control information" to enroll the user. *Id.* at 10:16-19, 10:45-63, 11:27-29 ("biometric signal 102 … is processed in order to provide access to the controlled item 111, or to take other action"). Limiting the claimed "biometric signal" to one that "provides secure access" ignores embodiments that use the biometric signal to "take other action," like enrolling the user, which the specification describes separately from and in contrast to "providing access to the controlled item." Such a construction is disfavored. *See Baxalta Inc. v. Genentech,*

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.