UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

VISA INC., and VISA U.S.A. INC.,[1]

Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,

Patent Owner.

Case IPR2018-00810

U.S. Patent No. 9,100,826

PETITIONER APPLE INC.'S SUR-REPLY TO PATENT OWNER'S REPLY TO THE OPPOSITION TO THE CONDITIONAL MOTION TO AMEND

[1] Visa Inc. and Visa U.S.A. Inc., which filed a petition in IPR2019-00175, have been joined as a party to this proceeding.

Contents

I. INTRODUCTION....1
II. ARGUMENT....1
A. Substitute Claim 56 Lacks Written Description Support Because The '860 Application Does Not Disclose Public/Private Key Encryption And Decryption.1
B. Schutzer And The '585 Reference Render Obvious The Digital Signature In Substitute Claims 36, 42, And 45. 3
C. The '585 Reference Would Have Motivated A POSITA To Use A Combination Function That Includes Prepending/Appending, Which Renders Obvious Substitute Claims 36, 42, And 45. 4
D. PO Does Not Overcome Petitioner's Showing That The KEK Architecture In Substitute Claim 56 Is Obvious. 8
E. The CMTA Opposition Explicitly Showed The Unpatentability Of Substitute Claim 45. 9
F. PO Fails To Overcome Petitioner's Showing That The Substitute Claims Are Patent Ineligible Under § 101....10
G. Patent Owner Has Not Satisfied Its Duty Of Candor....11
III. CONCLUSION 12
CERTIFICATE OF SERVICE 16

I. INTRODUCTION

In opposing the CMTA, Petitioner demonstrated that the plain text of the '860 application does not support substitute claim 56, that the incorporation of digital signatures in claim 36[f] was an obvious addition to a combined authentication code, and that encryption with a key-encryption-key was a well-known way to encrypt data. Patent Owner's ("PO") Reply does not dispute these points. Instead, PO resorts to introducing a new theory for written description support for claim 56 and mischaracterizing the teachings of the references cited by Petitioner, the testimony of Petitioner's experts, and the scope of claim 45. The Board should deny PO's CMTA.

II. ARGUMENT

A. Substitute Claim 56 Lacks Written Description Support Because The '860 Application Does Not Disclose Public/Private Key Encryption And Decryption.

The CMTA Opposition showed that substitute claim 56 lacks written description support for the claimed key-encryption-key ("KEK") architecture because the '860 application discloses at most an inoperable form of public-key encryption, which is unlike the use of symmetric keys in KEK encryption. CMTA Opp. at 3-4. PO and its expert now concede that – *as written* – the portions of the '860 application on which PO relies fail to support claim 56's KEK architecture. CMTA Reply at 4. Confronted with this admitted flaw, PO and its expert venture

the new argument that the Board should overlook the application's lack of disclosure because it reflects an "obvious error" and a POSITA would understand what was intended and "also readily recognize two corrections." CMTA Reply at 4-5; Ex-1017, Jakobsson Dep., 51:5-54:16. PO is wrong about this on all accounts.

First, a POSITA would not conclude that the application should be understood to mean what PO and Dr. Jakobsson belatedly claim. Ex-1019, Shoup-Decl., ¶¶27-28. PO now argues that a POSITA would recognize that pages 49-50 of the '860 application should be corrected in two ways: first, decrypting with a user's private, rather than public key, and second, changing both the encryption and decryption to be performed with a symmetric key. CMTA Reply at 4-5. But even Dr. Jakobsson, when deposed, did not suggest that a POSITA would identify both corrections. He identified only the first – which is the one that does not support the claimed KEK architecture. Ex-1017, Jakobsson-Dep., 51:5-55:16. And PO does not explain why a POSITA would understand a passage that discloses a single encryption technique to be corrected to one that discloses two alternative techniques, or why a disclosure limited to asymmetric public keys should be understood to disclose symmetric keys. Ex-1019, Shoup-Decl., ¶¶25-28.

Second, PO is incorrect that *In re Oda*, 443 F.2d 1200, 1205 (CCPA 1971), the sole case on which PO relies, would allow the Board to find written description support where the plain text of the '860 application provides none. Nothing in *Oda*

suggests that the specification may be "corrected" where, as here, it would not be evident to a POSITA what the correction would be. And PO presents no evidence as to why ***both*** asserted corrections are appropriate where the specification listed only one inoperable encryption technique. Furthermore, unlike in *Oda*, PO makes no argument as to the source of the error, much less that the source renders clear which correction is appropriate. *See* 443 F.2d at 1206 ("[I]t follows that when the nature of this error is known it is also known how to correct it."). Accordingly, PO fails to overcome Petitioner's showing that claim 56 lacks written description support.

B. Schutzer And The '585 Reference Render Obvious The Digital Signature In Substitute Claims 36, 42, And 45.

The CMTA Opposition demonstrates that Schutzer discloses a digital signature, and that it would have been obvious in view of the teachings of both Schutzer and the '585 reference to prepend or append a digital signature to the authentication code of the '585 reference. *See* CMTA Opp. at 8-10. PO does not dispute the obviousness of this combination, and instead tries to argue that Schutzer's digital signature is different from the claimed digital signature. CMTA Reply at 6-8. But that argument overlooks the detailed testimony of Dr. Shoup, who explained, citing Schutzer and the '585 reference, that it would have been obvious to include a digital signature that "securely authenticate authentication device user" to arrive at the limitations of claims 36, 42, and 45. *See* Ex-1019,

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.