Trials@uspto.gov
571-272-7822

Paper 49
Entered: February 7, 2023

PUBLIC VERSION

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NINTENDO CO., LTD., and NINTENDO OF AMERICA INC.,
Petitioner,

v.

ANCORA TECHNOLOGIES, INC.,
Patent Owner.

IPR2021-01338
Patent 6,411,941 B1

Before THU A. DANG, KEVIN W. CHERRY, and RYAN H. FLAX, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background

In response to a Petition (Paper 1, "Pet.") filed by Nintendo Co., Ltd. and Nintendo of America Inc. (collectively, "Petitioner"), we instituted *inter partes* review ("IPR") of claims 1−3, 6−14, and 16 ("the challenged claims") of U.S. Patent No. 6,411,941 B1 (Ex. 1001, "the '941 patent"). *See* Paper 9 ("Decision" or "Dec. Inst."). During the trial, Ancora Technologies, Inc. ("Patent Owner") filed a Response (Papers 22, 23, "PO Resp."), to which Petitioner filed a Reply (Papers 32, 33, "Pet. Reply."). In turn, Patent Owner filed a Sur-Reply. Papers 38, 39 ("PO Sur-Reply"). An oral hearing was held with the parties on October 3, 2022. A transcript of the hearing has been entered into the record. Paper 46 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has proven by a preponderance of the evidence that claims 1−3, 6−14, and 16 of the '941 patent are unpatentable.

B. The '941 patent

According to the '941 patent, software products have been developed to validate authorized software usage by writing a license signature onto the computer's volatile memory. Ex. 1001, 1:19–21. However, the '941 patent recognizes that these products are vulnerable to attack by "hackers" and the license signatures are "subject to the physical instabilities of their volatile memory media." *Id.* at 1:21–26. The '941 patent also recognizes that

hardware-based products developed to validate authorized software usage are "expensive, inconvenient, and not particularly suitable for software that may be sold by downloading." *Id.* at 1:27–32.

Thus, the '941 patent discloses a method of restricting software operation within a license limitation that relies on the use of a key and a record, which have been written into the non-volatile memory of a computer. *Id.* at 1:39–42. In particular, the method is applicable for a computer having a first non-volatile memory area, a second non-volatile memory area, and a volatile memory area (*see* below discussion of Figure 1). *Id.* at code (57). According to the '941 patent, the method includes the steps of selecting a program residing in the volatile memory, setting up a verification structure in the non-volatile memories, verifying the program using the structure, and acting on the program according to the verification. *Id.*

In a "specific non-limiting example," a conventional computer includes a conventional Basic Input / Output System ("BIOS") module in which a key constituting a unique identification code for the host computer was embedded at the read-only memory ("ROM") section thereof during manufacture, wherein the key is stored in a non-volatile portion of the BIOS where it cannot be removed or modified. *Id.* at 1:44–49. A verification structure is set in the BIOS so as to indicate that the specified program is licensed to run on the specified computer. *Id.* at 1:59–62. The encrypted license record is stored in another (second) non-volatile section of the BIOS, e.g., the electrically erasable programmable read-only memory ("EEPROM") section. *Id.* at 1:62–2:1. Unlike the first non-volatile section,

the data in the second non-volatile memory may be erased or modified so as to enable to add, modify or remove licenses. *Id.* at 2:1–5.

Figure 1 of the '941 patent is reproduced below.

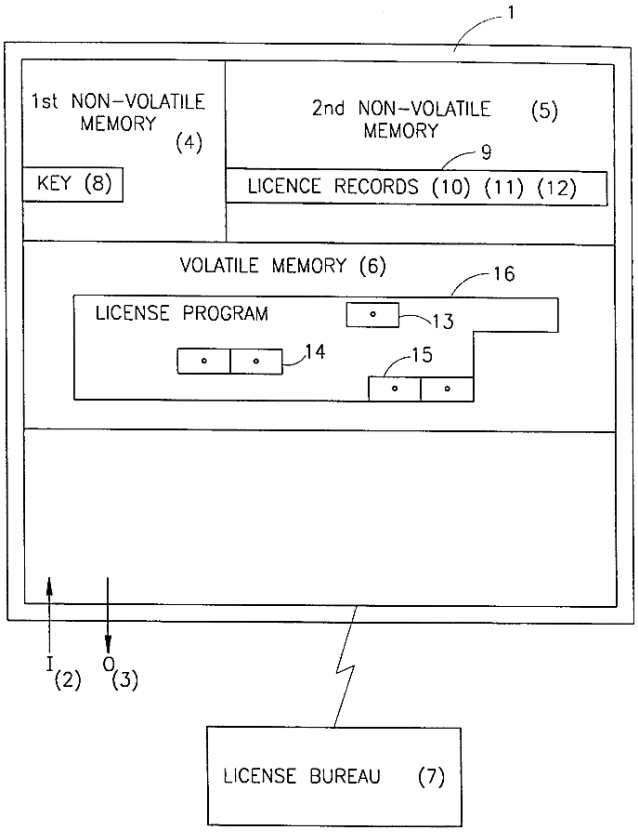

Figure 1 above shows a schematic diagram of computer processor 1 and license bureau 7. *Id*. at 5:9−16. Computer processor 1 is associated with input operations 2 and output operations 3. *Id*. Computer processor 1 contains first non-volatile memory area 4 (e.g., the ROM section of the BIOS), second non-volatile memory area 5 (e.g., the EEPROM section of the BIOS), and volatile memory area 6 (e.g., the internal random access memory ("RAM") of the computer). *Id*.

As shown in Figure 1, computer processor 1 is in temporary telecommunications linkage with license bureau 7. *Id.* at 5:17–18. The first

non-volatile memory includes pseudo-random identification key 8, which constitutes unique identification of the computer, and which exclusively or in combination with other information (e.g., user name), is sufficient to uniquely differentiate the first non-volatile memory from all other first non-volatile memories. *Id.* at 5:19–24. The second non-volatile memory includes license-record-area 9, which contains encrypted license records 10–12, and the volatile memory accommodates license program 16 having license record fields 1–15 appended thereto. *Id.* at 5:15–29.

C. The Challenged Claims

Of the challenged claims, only claim 1 is independent. Claims 2, 3, 6−14, and 16 directly or indirectly depend from claim 1.[1] Claim 1 is illustrative:

> 1. A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:
>
> selecting a program residing in the volatile memory,
>
> using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,
>
> verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and
>
> acting on the program according to the verification.

Ex. 1001, 6:59–7:4.

[1] Claims 4, 5, 15 and 17–19 are not challenged in this proceeding. *See generally* Pet.

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.