UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/563,410	09/21/2009	Christian Aabye	79900-758390 (043910US)	6347

66945 7590 03/30/2018

KILPATRICK TOWNSEND & STOCKTON LLP/VISA
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER
MILEF, ELDA G

ART UNIT	PAPER NUMBER
3694	

NOTIFICATION DATE	DELIVERY MODE
03/30/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipefiling@kilpatricktownsend.com
EDurrell@kilpatricktownsend.com
KTSDocketing2@kilpatrick.foundationip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CHRISTIAN AABYE,
HAO NGO, and
DAVID WILLIAM WILSON

Appeal 2016-000138
Application 12/563,410[1]
Technology Center 3600

Before HUBERT C. LORIN, SHEILA F. McSHANE, and
MATTHEW S. MEYERS, Administrative Patent Judges.

LORIN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Christian Aabye, et al. (Appellants) seek our review under 35 U.S.C. § 134 of the final rejection of claims 1–7, 9–12, 19–27, and 30–34. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

---

[1] The Appellants identify Visa International Service Association as the real party in interest. Appeal Br. 3.

SUMMARY OF DECISION

We AFFIRM and denominate the affirmance as a NEW GROUND OF REJECTION.

THE INVENTION

Claim 12, reproduced below, is illustrative of the subject matter on appeal.

> 12. A method of preventing unauthorized access to a payment application installed on a mobile payment device, comprising:
>
> determining, by the mobile payment device, that a user is attempting to utilize the payment application;
>
> in response to determining that the user is attempting to utilize the payment application, requesting the user to input user identification data;
>
> receiving the user identification data from a data input device that is part of the mobile payment device;
>
> verifying that the received user identification data is valid;
>
> using a trusted source controller or application programming interface (API) to obtain authentication data from a secret data store in response to verifying that the received user identification data is valid;
>
> providing the authentication data obtained from the secret data store to the payment application;
>
> authenticating the data input device of the mobile payment device as a trusted data input device at least in part by verifying the validity of the authentication data;
>
> providing the user with access to the payment application when both the authentication data and the user identification data are valid; and
>
> preventing the user from accessing the payment application when either the authentication data or the user identification data is not valid.

THE REJECTIONS

The Examiner relies upon the following as evidence of unpatentability:

Ritter	US 6,934,689 B1	Aug. 23, 2005
Labrou	US 2005/0187873 A1	Aug. 25, 2005
Kagan	US 2007/0078761 A1	Apr. 5, 2007
Dewe	WO 2007/145540 A2	Dec. 21, 2007

The following rejections are before us for review:

1. Claims 1–7, 9–12, 19–27, and 30–34 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.
2. Claims 1–7, 9, 11, 12, 19, 21–24, 26, 27, and 32–34 are rejected under 35 U.S.C. § 102(b) as being anticipated by Labrou.
3. Claims 10, 20, and 25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Ritter.
4. Claim 30 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Kagan.
5. Claim 31 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Dewe.

ISSUES

Did the Examiner err in rejecting claims 1–7, 9–12, 19–27, and 30–34 under 35 U.S.C. § 101 as being directed to non-statutory subject matter?

Did the Examiner err in rejecting claims 1–7, 9, 11, 12, 19, 21–24, 26, 27, and 32–34 under 35 U.S.C. § 102(b) as being anticipated by Labrou?

Did the Examiner err in rejecting claims 10, 20, and 25 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Ritter?

Did the Examiner err in rejecting claim 30 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Kagan?

Did the Examiner err in rejecting claim 31 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Dewe?

ANALYSIS

The rejection of claims 17, 9–12, 19–27, and 30–34 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

The Appellants argued these claims as a group. *See* Reply Br. 3–8. (There are separate headings for claims 12, 22, and 30 but the only argument presented is that "Appellant submits [the claims are] patent eligible for reasons similar to those discussed above [re claim 1]." Appeal Br. 13.) We select claim 1 as the representative claim for this group, and the remaining claims 2–7, 9–12, 19–27, and 30–34 stand or fall with claim 1. 37 C.F.R. § 41.37(c)(1)(iv).

Alice Corp. Proprietary Ltd. v. CLS Bank International, 134 S. Ct. 2347 (2014) identifies a two-step framework for determining whether claimed subject matter is judicially-excepted from patent-eligibility under 35 U.S.C. § 101.

According to *Alice* step one, "[w]e must first determine whether the claims at issue are directed to a patent-ineligible concept," such as an abstract idea. *Alice*, 134 S. Ct. at 2355.

In that regard, the Examiner determined the claims are "directed to authentication of a user accessing a payment application which is a

fundamental economic practice and thus an abstract idea." Final Act. 2. The Answer repeats much of what claim 1 recites and then characterizes that as a concept to which the claims are directed to, adding that "[t]his idea is similar to the basic concept of comparing new and stored information and using rules to identify options found to be an abstract idea by the courts, e.g., *SmartGene, Inc. v. Advanced Biological Labs., SA, 555 Fed. Appx. 950 (Fed. Cir. 2014).*" Ans. 3–4.

Step two is "a search for an 'inventive concept'—*i.e.,* an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 566 U.S. at 72–73).

In that regard, the Examiner determined that

> [t]he claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the claims are directed to an abstract idea with additional generic computer elements that do not add meaningful limitations to the abstract idea because they would be routine in any computer implementation.

Final Act. 2. The Answer says about the same, albeit again repeating much of what claim 1 recites. Ans. 3.

Claim 1 defines a mobile payment device. According to claim 1, said device comprises (a) "a processor programmed to execute a set of instructions"; (b) "a payment application installed in the mobile payment device"; (c) "a memory"; and (d) "[a] set of instructions stored in the memory [to be] executed by the processor [to] cause the mobile payment device [to perform functions]." These four elements, per se, are well known

and conventional. This is evidenced by the background discussion in the Specification with respect to consumer payment devices "used by millions of people worldwide to facilitate various types of commercial transactions" via, e.g., "smart" chips. Spec., paras. 2–9.

The invention lies not in the individual processor, payment application, memory, or instructions per se of the claimed device, or their ordered combination as claimed, but in the *specific* instructions that make up the "set of instructions" that claim 1 recites.

The specific instructions that make up the "set of instructions" that claim 1 recites perform two functions: (1) "[verification that a] received user identification data is valid" and (2) "[authentication of] a data input device of a mobile payment device as a trusted data input device at least in part by verifying the validity of the authentication data." Claim 1.

> With respect to (1), this is achieved by
>
> determin[ing] that a user is attempting to utilize the payment application installed in the mobile payment device;
>
> in response to determining that the user is attempting to utilize the payment application, request[ing] the user to input user identification data;
>
> receiv[ing] the user identification data from a data input device that is part of the mobile payment device; [and]
>
> verify[ing] that the received user identification data is valid.

Claim 1. This verification scheme reasonably broadly covers the commonplace input and validation of one's user identification (ID) and password before an application can be accessed. *See* Spec. para. 8.

> If (1) is successfully accomplished, then (2) is performed.
>
> With respect to (2), this is achieved by

> obtain[ing] authentication data from a secret data store [via a trusted source controller or application programming interface (API)];
>
> provid[ing] the authentication data obtained from the secret data store to the payment application; [and,]
>
> verifying the validity of the authentication data [, thereby authenticating the data input device of the mobile payment device as a trusted data input device].

Claim 1.

This verification scheme (2) calls for the use of a "trusted source controller or application programming interface (API)." Controllers/APIs are not disclosed to be anything other than conventional software performing the steps as claimed. *See* Spec. para. 49. This scheme calls for using such known elements to obtain authentication data from a "secret data store" and then to provide said data to the payment application. Then the authentication data is validated.

If (1) and (2) are successful, then "the user [gains] access to the payment application" (claim 1). Otherwise, access is denied.

In effect, claim 1 combines two authentication schemes, both of which are required to be successfully validated in order to provide a user with access to a payment application of a mobile payment device. The first reasonably broadly covers the common verification of one's ID and password. The second – which is conducted if validation of the first authentication scheme is successful — obtains authentication data from a "secret data store," provides it to the payment application, and validates it.

It is the addition of a second authentication which is the focus of the claimed advance over the prior art. "The 'abstract idea' step of the inquiry calls upon us to look at the 'focus of the claimed advance over the prior art'

to determine if the claim's 'character as a whole' is directed to excluded subject matter.'" *Affinity Labs of Texas v. DirectTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) (*quoting Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016); *see also Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016). The Specification supports this view. *See* e.g.,

> [0006] In a typical payment transaction, data is sent from a point of sale terminal to the Issuer to authenticate a consumer and obtain authorization for the transaction.
>
> [0007] A payment device may include a payment application which is activated in order to enable a consumer to initiate or otherwise conduct a payment transaction. . . . A potential security problem that may arise with such payment devices is that an unauthorized person may try to obtain access to the payment application or to transaction data by using the wireless network communications ability of the payment device to activate the payment application or to attempt to access data stored in a secure memory of the payment device.
>
> [0010] . . . The invention prevents unauthorized access . . . by requiring that access control data be received from a trusted source, such as a controller or application in charge of managing inputs from a phone keypad, in order to activate the payment application or to access stored data.

Step one. In our view, claim 1 is directed to a dual-authentication scheme. The claim's character as a whole is directed to adding an additional authentication to that commonly required to access an application.

Authentication, per se, is an abstract idea. *See EasyWeb Innovations, LLC v. Twitter, Inc.*, 2016 WL 1253674 (E.D.N.Y. 2016), aff'd, No. 2016-2335 (Fed. Cir. 2017) ("receiving, authenticating, and publishing data" is an abstract idea.) Claims that include authentication steps have been found

patent ineligible. *See* e.g., *Intellectual Ventures I LLC v. J. Crew Group, Inc.*, 703 Fed. Appx. 991 (Mem.) (Fed. Cir. 2017); *Front Row Technologies LLC v. MLB Advanced Media, L.P.*, 2017 WL 4127880 (Mem.) (Fed. Cir. 2017); *GoDaddy.com LLC v. RPost Communications Limited*, 2017 WL 1829147 (Mem.) (Fed. Cir. 2017); *Clarilogic, Inc. v. FormFree Holdings Corporation*, 2017 WL 992528 (Fed. Cir. 2017); *Morsa v. Facebook, Inc.*, 622 Fed.Appx. 915 (Mem.) (Fed. Cir. 2015); and, *Prism Technologies LLC v. T-Mobile USA, Inc.*, 696 Fed. Appx. 1014 (Fed. Cir. 2017).

Based on these earlier decisions it is reasonable to find dual-authentication to be similarly an abstract idea. "[T]he decisional mechanism courts now apply is to examine earlier cases in which a similar or parallel descriptive nature can be seen—what prior cases were about, and which way they were decided." *Amdocs (Israel) Limited v. Openet Telecom, Inc.* 841 F.3d 1288, 1294 (Fed. Cir. 2016).

The Appellants disagree that claim 1 is directed to an abstract idea. According to the Appellants, "it is self-evident that the claims are patent eligible." Appeal Br. 10. According to the Appellants,

> claim 1 recites "*use a trusted source controller or application programming interface (API) to obtain authentication data from a secret data store in response to verifying that the received user identification data is valid; ... authenticate the data input device of the mobile payment device as a trusted data input device at least in part by verifying the validity of the authentication data; ... provide the user with access to the payment application when both the authentication data and the user identification data are valid ...*"

(Appeal Br. 1) which is "not [ ] a fundamental economic practice known from the pre-Internet world, but instead recite[s] a solution to a problem

necessarily rooted in computer technology" (Appeal Br. 10). According to the Appellants,

> authentication of a user accessing a payment application on a mobile device is a concept that has only came into existence in recent years. With advances in the computing power of mobile devices in recent years, mobile devices can now be installed with a payment application to allow the mobile device to be used as a payment instrument for contactless transactions. As explained in the Summary of the Claimed Subject Matter, one problem with such a mobile device is that an unauthorized party may attempt to connect to the mobile device via the wireless network capabilities of the mobile device and gain access to the payment application. To prevent wireless hacking into the payment application of the mobile device, the claims recite techniques that utilize two levels of authentication that not only authenticates the user based on user identification data, but also [the] authenticates the data input element of the mobile device receiving the user identification data.
>
> Appellant submits that preventing wireless hacking into a mobile device is not a concept directed to a fundamental economic practice, but is instead a concept inextricably tied to computer technology arising in the realm of wireless computer networks.

Appeal Br. 9. The Appellants also argue that "the claims recite a very specific way of preventing access to a payment application that clearly do not seek to preempt others from performing the alleged abstract idea of authenticating a user accessing a payment application using other techniques." Appeal Br. 10.

The argument is unpersuasive because the claim is more broadly directed to dual-authentication.

The Appellants' pre-emption argument confuses the pre-emption concern with levels of abstraction. "What matters is whether a claim threatens to subsume the full scope of a fundamental concept, and when

those concerns arise, we must look for meaningful limitations that prevent the claim as a whole from covering the concept's every practical application." *CLS Bank Intern. v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1281 (Fed. Cir. 2013) (Lourie, J., concurring). Here the argued-over "very specific way of preventing access to a payment application" (Appeal Br. 10) simply describes the dual-authorization abstract idea at a lower level of abstraction. It does not render the dual-authorization abstract idea to which the claim is directed to any less an abstract idea.

> To be clear, the proper focus is not preemption *per se*, for some measure of preemption is intrinsic in the statutory right granted with every patent to exclude competitors, for a limited time, from practicing the claimed invention. See 35 U.S.C. § 154. Rather, the animating concern is that claims should not be coextensive with a natural law, natural phenomenon, or abstract idea; a patent-eligible claim must include one or more substantive limitations that, in the words of the Supreme Court, add "significantly more" to the basic principle, with the result that the claim covers significantly *less*. See Mayo 132 S. Ct. at 1294. Thus, broad claims do not necessarily raise § 101 preemption concerns, and seemingly narrower claims are not necessarily exempt.

Id. See also Ariosa Diagnostics, Inc. v. Sequenom, Inc., 788 F.3d 1371, 1379 (Fed. Cir. 2015) ("[w]hile preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility.").

Since we find the claimed subject matter covers patent-ineligible subject matter, the pre-emption concern is necessarily addressed. "Where a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, [] preemption concerns are fully addressed and made moot." *Ariosa Diagnostics*, 788 F.3d at 1379.

Step two. The Appellants argue that

> [i]n the present case, Appellant submits that the claims are patent eligible under the second part of the *Mayo* test, because the claims, as a whole, improve another technology or technical field as well as improve the functioning of the computer itself. . . . Preventing unauthorized access to an application installed on a mobile device is a computer security related concept, and thus the claimed techniques provide improvements to technical field of computer security by mitigating wireless hacking of the application installed on a mobile device. Furthermore, because the claimed techniques enhances the security protection of the mobile device, the claims also improve the functioning of the mobile device itself by making the application installed on the mobile device more secure and less susceptible to unauthorized access.

Appeal Br. 11–12.

As we already stated, claim 1 is directed more broadly to dual-authentication and is not limited to overcoming wireless hacking. The claimed technique does not provide improvements in the technical field of computer security by mitigating wireless hacking of the application installed on a mobile device. Rather, claim 1 more broadly covers a mobile payment device performing dual-authentication.

There is no dispute that the elements of the claimed device which practice the claimed dual-authentication scheme are conventional. Given the intrinsic evidence, we do not see, and the Appellants do not explain, how the mobile payment device is improved by practicing said scheme. The individual elements are conventional and they perform as they are expected to. Their ordered combination as claimed does no more than what they are expected to do individually. *Cf. Prism Technologies LLC v. T-Mobile USA, Inc.*, 696 Fed. Appx. 1014, 1017 (Fed. Cir. 2017):

> The asserted claims merely recite a host of elements that are indisputably generic computer components. … Viewed as an ordered combination, the asserted claims recite no more than the sort of "perfectly conventional" generic computer components employed in a customary manner that we have previously held insufficient to transform the abstract idea into a patent-eligible invention. *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1321 (Fed. Cir. 2016).

The dual-authentication of claim 1 lacks the necessary details as to, for example, any non-conventional software to transform it into an inventive concept. *Cf. Credit Acceptance Corp.,* 859 F.3d at 1057.

> Significantly, the claims do not provide details as to any non-conventional software for enhancing the financing process. *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1342 (Fed. Cir. 2017) (explaining that "[o]ur law demands more" than claim language that "provides only a result-oriented solution, with insufficient detail for how a computer accomplishes it"); *Elec. Power Grp.*, 830 F.3d at 1354 [*Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016)]; (explaining that claims are directed to an abstract idea where they do not recite "any particular assertedly inventive technology for performing [conventional] functions").

For the foregoing reasons, the rejection is affirmed. However, to the extent our reasoning departs from that of the Examiner, we denominate the affirmed rejection as a new ground of rejection.

The rejection of claims 1–7, 9, 11, 12, 19, 21–24, 26, 27, and 32–34 under 35 U.S.C. § 102(b) as being anticipated by Labrou.

All the claims require "using a trusted source controller or application programming Interface (API) to obtain authentication data from a secret data store in response to verifying that the received user identification data is valid." Claim 12. Similar language is used in the other independent claims,

claims 1 and 22. The Examiner (Final Act. 4) cites para. 87 of Labrou as evidence that said claim limitation is expressly described in the prior art, which reads as follows:

> [0087] As shown in the **FIG. 4**, a view **402** comprises a cipher text part (or encrypted part) **406** and a perceptible (e.g., plaintext) part **408**. A plain text part **408** includes the TID, the DIDc of the payer **200** generating the view **402**, and the local current timestamp (TS) of device **106**. The TS, among other functions described herein, is also used to prevent transaction replay. The encrypted part **406** includes two critical fields: the agreement data and the DIDm of the payee's **202** device **106** involved in the agreement. The DIDm is the minimum necessary reference field in order to provide the desired verification properties of the UPTF protocol. Therefore, a user can execute a UPTD **106** cashless monetary transaction with a transaction party according to a PIE and a wireless wallet software **108** authentication parameter RSN and transaction messages comprising an identifier of the mobile phone, an identifier of the transaction party and an identifier for a transaction (for example, an identifier and/or other transaction related data such as payment amount, etc.) thereby providing the UPTD wireless wallet based upon a combination of the mobile payment software at the UPTD and STS association of the PIE and the software authentication parameter with financial entities of the user and exchange of the transaction messages between the user, the transaction party and the STS **120**.

The Examiner does not clearly explain what in para. 87 of Labrou corresponds to a trusted source controller or application programming Interface (API); authentication data; or a secret data store. The Appellants understand the Examiner to be equating Labrou's "RSN" to the claimed authentication data. Appeal Br. 14. The Examiner appears to agree with that. *See* Ans. 4. Assuming that is the case, we agree with the Appellants that Labrou does not further describe the limitation "using a trusted source controller or application programming Interface (API) to obtain [said]

authentication data from a secret data store in response to verifying that the received user identification data is valid" (claim 12).

According to said claim limitation, in response to verifying that the received user identification data is valid, a trusted source controller or API obtains authentication data from a secret data store. Thus, consistent with equating Labrou's "RSN" to the claimed authentication data, Labrou would have to describe a trusted source controller or API obtaining the RSN from a secret data store in order for Labrou to anticipate the claimed subject matter. We have reviewed para. 87 and are unable to find disclosure describing obtaining the RSN from a secret data store, let alone "in response to verifying that the received user identification data is valid."

For the foregoing reasons, after our consideration of the Appellants' arguments and the evidence presented in this Appeal for the § 102 rejection, we are persuaded that the Appellants identify reversible error, and we therefore reverse the anticipation rejection.

The rejection of claims 10, 20, and 25 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Ritter.

The rejection of claim 30 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Kagan.

The rejection of claim 31 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Dewe.

These rejections rely on the fact that Labrou expressly describes "using a trusted source controller or application programming Interface (API) to obtain authentication data from a secret data store in response to verifying that the received user identification data is valid." Claim 12. *See* also claims 1 and 22. For the reasons discussed above, a preponderance of

the evidence does not support said finding of fact. Accordingly, after our consideration of the Appellants' arguments and the evidence presented in this Appeal for the § 103 rejection, we are persuaded that the Appellants identify reversible error, and we therefore reverse the anticipation rejection.

CONCLUSIONS

The rejection of claims 1–7, 9–12, 19–27 and 30–34 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is affirmed but denominated as a new ground of rejection.

The rejection of claims 1–7, 9, 11, 12, 19, 21-24, 26, 27, and 32–34 under 35 U.S.C. § 102(b) as being anticipated by Labrou is reversed.

The rejection of claims 10, 20, and 25 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Ritter is reversed.

The rejection of claim 30 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Kagan is reversed.

The rejection of claim 31 under 35 U.S.C. § 103(a) as being unpatentable over Labrou and Dewe is reversed.

DECISION

The decision of the Examiner to reject claims 1–7, 9–12, 19–27, and 30–34 is affirmed, but the affirmed rejection under §101 is denominated as a new ground of rejection.

NEW GROUND

This decision contains a new ground of rejection pursuant to

37 C.F.R. § 41.50(b). 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review." 37 C.F.R. § 41.50(b) also provides that the Appellants, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> (1) *Reopen prosecution.* Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the prosecution will be remanded to the examiner. . . .
>
> (2) *Request rehearing.* Request that the proceeding be reheard under § 41.52 by the Board upon the same Record. . . .

Should the Appellants elect to prosecute further before the Examiner pursuant to 37 C.F.R. § 41.50(b)(1), in order to preserve the right to seek review under 35 U.S.C. §§ 141 or 145 with respect to the affirmed rejection, the effective date of the affirmance is deferred until conclusion of the prosecution before the Examiner unless, as a mere incident to the limited prosecution, the affirmed rejection is overcome.

If Appellants elect prosecution before the Examiner and this does not result in allowance of the application, abandonment or a second appeal, this case should be returned to the Patent Trial and Appeal Board for final action on the affirmed rejection, including any timely request for rehearing thereof.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED
37 C.F.R. § 41.50(b)