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.
14/065,355	10/28/2013	Nathan Moore	5679	1087

21834 7590 01/06/2020

Tysver Beck Evans, PLLC
225 S. 6th Street, Suite 1750
Minneapolis, MN 55402

EXAMINER	
ALLADIN, AMBREEN A	

ART UNIT	PAPER NUMBER
3693	

NOTIFICATION DATE	DELIVERY MODE
01/06/2020	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):

docket@bitlaw.com
dtysver@bitlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte NATHAN MOORE, JIANING CHEN,
JIM RANSCO II, and JOHN DILLON

Appeal 2019-002697
Application 14/065,355
Technology Center 3600

Before JEFFREY N. FREDMAN, RACHEL H. TOWNSEND, and MICHAEL A. VALEK, *Administrative Patent Judges*.

FREDMAN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal[1,2] under 35 U.S.C. § 134(a) involving claims to a method of authentication and resource allocation. The Examiner rejected the claims as indefinite, as obvious, and as reciting non-statutory subject matter. We have jurisdiction under 35 U.S.C. § 6(b). We affirm the obviousness rejection.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the Real Party in Interest as Cash Flow Management, Inc. (*see* App. Br. 3).

[2] We have considered and herein refer to the Specification of Oct. 28, 2013 ("Spec."); Final Office Action of Sept. 18, 2018 ("Final Act."); Appeal Brief of Oct. 31, 2018 ("App. Br."); Examiner's Answer of Dec. 20, 2018 ("Ans."); and Reply Brief of Feb. 20, 2019 ("Reply Br.").

Statement of the Case

Background

"Banks and credit unions are constantly looking for ways to reduce the time their staff spend on routine transactions and increase the time they spend on engaging with . . . their customers" (Spec. ¶ 3). "It has helped the teller focus more on the customer and less on the cash as the automation is handling the counting, tracking and balancing for them" (*id.* ¶ 4).

The Claims

Claims 26–35 are on appeal. Independent claim 26 is representative and reads as follows:

> 26. A method of authentication and resource allocation comprising
> a) at a computer server, receiving from a mobile device communications relating to a first secure transaction, the first secure transaction comprising a plurality of actions including accessing one of a plurality of hardware devices;
> b) at the computer server, communicating with the mobile device to complete all the actions in the first secure transaction other than the accessing one of the plurality of hardware devices, wherein the hardware devices are capable of being controlled by an external computing device;
> c) at the computer server, generating an authentication token for the first secure transaction;
> d) at the computer server, storing secure transaction details for the first secure transaction in a resource request database accessible by all of the plurality of hardware devices, the secure transaction details being associated with the authentication token;
> e) at the computer server, transmitting the authentication token to the mobile device;
> f) at a first hardware device of the plurality of hardware devices, receiving the authentication token from the mobile device;

> g) at the first hardware device, requesting and receiving the secure transaction details from the resource request database;
> h) at the first hardware device, verifying the authentication token against the received secure transaction details; and
> i) at the first hardware device, using the secure transaction details to complete the secure transaction.

The Rejections

A. The Examiner rejected claims 26–35 under 35 U.S.C. § 112(b) as indefinite (Final Act. 2–3).

B. The Examiner rejected claims 26–35 under 35 U.S.C. § 103 as obvious over Labrou[3] (Final Act. 25–30).

C. The Examiner rejected claims 26–35 under 35 U.S.C. § 101 as directed to an abstract idea (Final Act. 3–25).

A. 35 U.S.C. § 112(b)

The Examiner finds

> there is a disconnect between the preamble and the body of the claim. Specifically, the preamble states "a method of authentication and resource allocation comprising" while the claim ends with a recitation of . . . "using the secure transaction details to complete the secure transaction". The claim does not actually complete the action of "resource allocation."

(Final Act. 2–3).

Appellant responds "[t]his preamble does not make the claim less distinct, nor does the claim fail to particularly point out the invention. There is no disconnect, and, even if any were present, such disconnect does not rise to a violation of the requirements of Section 112" (App. Br. 19–20).

---

[3] Labrou et al., US 2006/0206709 A1, published Sept. 14. 2006.

MPEP § 2173.05(e)(III) states "[t]he mere fact that the body of a claim recites additional elements which do not appear in the claim's preamble does not render the claim indefinite under 35 U.S.C. 112(b)." "[H]ow much clarity is required necessarily invokes some standard of reasonable precision in the use of language in the context of the circumstances." *In re Packard*, 751, F.3d 1307, 1313 (Fed. Cir. 2014).

In this case, we agree with Appellant that the ordinary artisan would understand the limitations of claim 26 as functioning to perform authentication and resource allocation, as recited in the preamble, using the authentication token process and resource request database recited in the claim. In particular, step(g) of claim 26 requires a hardware device to function in "requesting and receiving the secure transaction details from the resource request database." This step therefore requires a resource allocation of transaction details from a resource request database and is reasonably understood as addressing the limitation in the preamble. There is no requirement for *ipsis verbis* repetition of preamble language.

B. 35 U.S.C. § 103 over Labrou

The Examiner finds Labrou teaches the limitations of claim 26 and finds "Labrou discloses that it is generally understood that a user will have to fulfill the ATM transaction at the ATM within a specified period of time that was authorized through the mobile phone" (Final Act. 28). The Examiner acknowledges that "Labrou does not directly disclose that the transaction is reversed if the completion report is not received within a predetermined period though it is implied that the transaction would not be completed if the specified time period expired" (*id.*).

> The Examiner finds it obvious
>
> that not fulfilling a previously authorized transaction at the ATM within a specified time period would result in a reversal of the authorization at the expiry of the time period as it is within the capabilities of one of ordinary skill in the art at the time the invention was made to modify Labrou with the predicted result of a reversal if the time period for performing an authorized transaction expired.

(Final Act. 28).

> Appellant responds
>
> that the Labrou reference fails to teach the following elements of the claim:
>
> - (d) at the computer server, storing secure transaction details for the first secure transaction in a resource request database accessible by all of the plurality of hardware devices, the secure transaction details being associated with the authentication token;
> - (g) at the first hardware device, requesting and receiving the secure transaction details from the resource request database;
> - (h) at the first hardware device, verifying the authentication token against the received secure transaction details; and
> - (i) at the first hardware device, using the secure transaction details to complete the secure transaction.

(App. Br. 17–18).

We note that Appellant does not argue the claims separately, so claims 27–35 stand or fall with claim 26 because separate reasons for their patentability were not provided in the Appeal Brief. 37 C.F.R. § 41.37(c)(1)(iv).

The issue with respect to this rejection is: Does the evidence of record support the Examiner's conclusion that Labrou renders the claims obvious?

Findings of Fact

1. Labrou teaches

> A method, and an apparatus performing the method, is provided by authenticating a mobile device communicably connectable to a wireless network by an authentication parameter from a secure transaction server (STS), as a mobile device authenticator; providing an STS correlation between a personal identification entry (PIE) and the mobile device authenticator; and inputting, by a user, the PIE and a provider action, to the mobile device authenticator to transmit a transformed secure user authenticable authorization request to the STS over the wireless network to authorize an action with a provider.

(Labrou ¶ 11).

2. Figure 1 of Labrou is reproduced below:

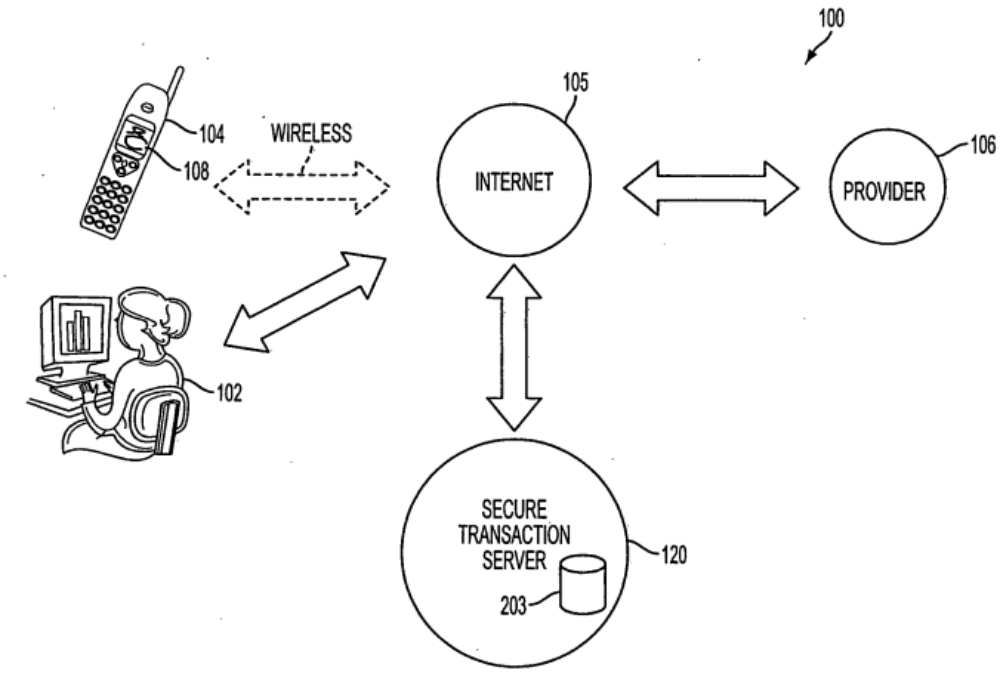

FIG. 1

FIG. 1 is a diagram of a computer system **100** to provide mobile device authentication services . . . a user **102** uses a mobile wireless device **104** for authentication. The mobile

> wireless device **104** is any mobile wireless computing device or mobile radio computing device, including, without limitation, a mobile phone, that wirelessly communicates (e.g., wireless Internet **105** or mobile phone network) to a secure transaction server **120**.

(Labrou ¶ 32).

3. Labrou teaches a two-factor authentication process for banking in which:

> the user starts the mobile ID application **108** on the mobile phone **104**, selects the provider (e.g., Bank) and the action to authorize (e.g., log in) and then enters the user's PIN. At operation **506**, the mobile ID application **108** generates and sends a UPTF message to the STS **120**. At operation **508**, the STS **120** compares the mobile phone's message to the previously received message f[ro]m the provider **106**, and if the two messages agree, the STS **102** responds positively to the provider **106**. At operation **510**, the provider **106**, upon receiving a positive response, approves the user's login request and authorizes the user's access to user's account and proceeds to display to the user a webpage with the user's account information. Therefore, the mobile device authenticator **104** is a second factor authentication in addition to the first factor user's username and password entered at the website.

(Labrou ¶ 78).

4, Labrou teaches authentication at an automated teller machine (ATM) in which "the ATM **106** requests, via a UPTF message **404** (request transaction token), from the STS **120** a Transaction Token" after which "the ATM receives a response UPTF message **404** from the STS **120** with a specific Transaction Token" (Labrou ¶ 109).

5. Labrou teaches that the server "STS **120** verifies the UPTF user authorize transaction message **402** of operation **910** against the ATM

authorize transaction message **404** of operation **908** or against the request token transaction message at operation **906**" (Labrou ¶ 109).

6. Labrou teaches an embodiment where an

> ATM transaction authorized through the mobile phone **104** will be fulfilled or completed whenever the user can interact with the ATM. . . .
>
> the user **102** stands in the area of the ATM **106** prior to interacting with the ATM user interface, perhaps waiting in line. The ATM posts (physically), a number ATM_ID **922** (in a visible area, say next to its logo) that uniquely identifies this particular ATM. The STS **120** knows this ATM by that ATM identifying number. It is also possible that the ATM is automatically determined by the location of the user, for example, if the mobile phone **104** is equipped with GPS or location capabilities . . .
>
> Then, at operation **924**, the user **102** starts the mobile ID authentication application **108** on their mobile **104**, and, optionally, enters in the application **108**, the ATM identifier, such as the number the user sees on the ATM (ATM_ID **922**).

(Labrou ¶¶ 111–112).

7. Labrou teaches that after the ATM identifier is in the mobile ID authentication application:

> the STS **120** sends to the ATM identified by ATM_ID a message that identifies the user that attempts to interact with the ATM and the details of the requested transaction and a Transaction Token used to refer to this specific transaction. The ATM determines if the ATM can indeed perform the requested transaction for the specified user, and if determined positively, at operation **928**, the ATM sends to the STS **120** an ATM authorize transaction UPTF message **404** for the transaction identified by the transaction token. The STS **120** verifies the UPTF user authorize transaction message **402** against the ATM authorize transaction message **404**, and the STS **120**, at

> operations **930**, **932**, upon a successful verification transmits a confirmation code to the mobile device **104** and the ATM **106**. Once the user is physically present at the ATM to interact with the user interface of the ATM **106**, the user must enter the confirmation code at the ATM to complete the transaction. . . .
>
> after which the ATM will simply execute the previously authorized transaction

(Labrou ¶¶ 112–113).

8. Labrou teaches an embodiment where "[w]hen the user approaches the ATM, she waves a Near Field Communication (NFC)-enabled phone to the NFC-enabled ATM which responds by executing the previously requested transaction" (Labrou ¶ 115).

Principles of Law

"The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

Analysis

We adopt the Examiner's findings of fact and reasoning regarding the scope and content of the prior art (Final Act. 25–30; FF 1–8) and agree that the claims are obvious over Labrou. We address Appellant's arguments below.

Appellant contends that the "key distinction between Labrou and the present claims is that the user in Labrou (the mobile device) must be linked to a specific ATM" while "the pending claims describe a method that allows a user to use any of a plurality of hardware devices that can be selected at a later time when the process is to be completed" (App. Br. 17). Appellant contends, regarding step (d) of claim 26, that Labrou does "not teach the

storage of transaction details in any type of database in association with the authentication token, let alone a database accessible by the plurality of hardware devices" (App. Br. 18).

We find this argument unpersuasive because, as the Examiner points out, claim 26 step (d) simply requires "a resource request database accessible by all of the plurality of hardware devices." Labrou clearly teaches a resource request database, specifically the secure transaction server (FF 1). Labrou teaches that the STS is accessible to a plurality of ATMs because if only a single ATM was connected, there would be no need for "a number ATM_ID **922** . . . that uniquely identifies this particular ATM" (FF 6).

To the extent that Appellant is arguing that claim 26 encompasses the situation where the transaction is first performed and then the user selects a particular device, such as an ATM, with which to transact, we agree with the Examiner that this language is not in the claims (*see* Ans. 35). *See In re Self*, 671 F.2d 1344, 1348 (CCPA 1982) ("[A]ppellant's arguments fail from the outset because . . . they are not based on limitations appearing in the claims."). We note that Appellant acknowledges that "language concerning later selection is not found in the claims" (Reply Br. 4).

Finally, Labrou teaches that the "STS **120** knows this ATM by that ATM identifying number" (FF 6). Labrou's use of the phrase "this ATM" reasonably suggests that in locations where multiple ATMs are present, it would have been obvious for the STS to authenticate use at whichever ATM was selected by the user, through entry of the ATM identifying number (FF 6) or by near field communication (FF 8), to allow the user selected ATM to respond "by executing the previously requested transaction" (FF 8).

Appellant contends that "Labrou fails to teach these steps g, h, and i of claim 26" (App. Br. 19). Appellant contends that:

> The hardware device in Labrou does not request and receive secure transaction details from the resource request database, as Labrou does not even store the transaction details in a database. Furthermore, the ATM in Labrou does not request transaction details from a central storage area. In Labrou, the ATM is provided these details at the beginning of the transaction, and therefore does not need to request those details at a later time. Furthermore, because transaction details were not stored in a resource request database that was accessible by many hardware devices, Labrou cannot be considered to use the type of transaction details specified in the claims compare to the authentication token (step h) or to complete the secured transaction (step i).

(App.Br. 19).

We are not persuaded. As to step (g) of claim 26, Labrou teaches that after the user identifies the ATM, the first hardware device (FF 6), "the STS **120** sends to the ATM identified by ATM_ID a message . . . and the details of the requested transaction and a Transaction Token used to refer to this specific transaction" (FF 7). Then "the ATM sends to the STS **120** an ATM authorize transaction UPTF message **404** for the transaction identified by the transaction token" (FF 7). Thus, Labrou teaches that the ATM requests and receives the secure transaction details from the STS (secure transaction server). We agree with the Examiner that these teachings in Labrou reasonably suggest the step of "requesting and receiving the secure transaction details from the resource request database" as required by step (g) of claim 26.

As to step (h) of claim 26, as noted above, Labrou teaches the "ATM determines if the ATM can indeed perform the requested transaction for the

specified user, and if determined positively, at operation **928**, the ATM sends to the STS **120** an ATM authorize transaction UPTF message **404** for the transaction identified by the transaction token" (FF 7). Labrou then teaches "upon a successful verification transmits a confirmation code to the mobile device **104** and the ATM **106**" (FF 7). Thus, the ATM or first hardware device compares the transaction requirements with the transaction token provided by the secure transaction server, verifying that the ATM can perform the requested transaction. We agree with the Examiner that these teachings of Labrou reasonably suggest the step of "verifying the authentication token against the received secure transaction details" as required by step (h) of claim 26.

Lastly, as to step (i) of claim 26, Labrou teaches "[o]nce the user is physically present at the ATM to interact with the user interface of the ATM **106**, the user must enter the confirmation code at the ATM to complete the transaction. . . . after which the ATM will simply execute the previously authorized transaction" (FF 7). Thus, the ATM uses the secure transaction details previously authorized by the secure transaction server in combination with the ATM and completes the transaction. We agree with the Examiner that these teachings of Labrou reasonably suggest the step of "using the secure transaction details to complete the secure transaction" as required by step (i) of claim 26.

Conclusion of Law

The evidence of record supports the Examiner's conclusion that Labrou renders the claims obvious.

C. 35 U.S.C. § 101

The Examiner finds the claims "are directed to the abstract idea of processing of secure transactions using authentication tokens via a series of steps" (Final Act. 3). The Examiner finds this abstract idea is "directed to the performance of certain financial transactions" and is a "method of organizing human activity" (*id* at 4).

Appellant contends:

> The character of the present claims relates to the use of an authentication token and resource request database to securely transfer a transaction, begun between two computer devices, to a third hardware device for completion of the transaction. This clearly represents an increase in security and efficiency in computer communications, and hence represents a specific improvement to the way computers operate.

(App. Br. 9).

Principles of Law

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. However, the Supreme Court has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *See, e.g.*, *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Supreme Court's two-step framework, described in *Mayo* and *Alice*. *Id.* at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of

intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk.").

Concepts determined to be abstract ideas, and therefore patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611) and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 69 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as "molding rubber products" (*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)) or software "purporting to improve the functioning of the computer itself" (*Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016)).

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (quotation marks omitted). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

The United States Patent and Trademark Office published revised guidance on the application of 35 U.S.C. § 101. USPTO's *2019 Revised*

Patent Subject Matter Eligibility Guidance ("Revised Guidance").[4] Under the Guidance, in determining what concept the claim is "directed to," we first look to whether the claim recites:

> (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity such as a fundamental economic practice, or mental processes) (Guidance Step 2A, Prong 1); and
>
> (2) additional elements that integrate the judicial exception into a practical application (*see* MPEP § 2106.05(a)–(c), (e)–(h)) (Guidance Step 2A, Prong 2).

Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then look to whether the claim contains an "'inventive concept' sufficient to 'transform'" the claimed judicial exception into a patent-eligible application of the judicial exception. *Alice*, 573 U.S. at 221 (quoting *Mayo*, 566 U.S. at 82). In so doing, we thus, consider whether the claim:

> (3) adds a specific limitation beyond the judicial exception that are not "well-understood, routine and conventional in the field" (*see* MPEP § 2106.05(d)); or
>
> (4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.
>
> (Guidance Step 2B). *See* Guidance, 84 Fed. Reg. at 54–56.

Analysis

Applying the Revised Guidance to the facts on this record, we find that Appellant's claims 26–35 are directed to patent-eligible subject matter.

---

[4] *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50–57 (January 7, 2019).

Because the same issues are present in each of the claims, we focus our consideration on representative claim 26. The same analysis applied below to claim 26 also applies to the other rejected claims.

A. Guidance Step 2A, Prong 1

The Revised Guidance instructs us first to determine whether any judicial exception to patent eligibility is recited in the claim. The Revised Guidance identifies three judicially-excepted groupings identified by the courts as abstract ideas: (1) mathematical concepts, (2) certain methods of organizing human behavior such as fundamental economic practices, and (3) mental processes.

Claim 26 reasonably falls within one of the three of the judicially-excepted groupings listed in the Revised Guidance: fundamental economic practices involving authenticating financial transactions. *Alice* found an abstract idea in claims to "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Alice*, 573 U.S. at 219. Claim 26 recites a method of authentication where tokens are exchanged to determine if a particular transaction is authorized or not. This is reasonably understood as a fundamental economic practice, just as a bank teller requires tokens of authentication such as a driver's license or ATM card prior to dispensing money to a customer. Accordingly, we conclude that the steps of claim 26 recites the judicial exception of organizing human activities.

B. Guidance Step 2A, Prong 2

Having determined that the claims recite a judicial exception, the Revised Guidance directs us to next consider whether the claims integrate

the judicial exception into a practical application. Guidance Step 2A, Prong 2. "[I]ntegration into a practical application" requires that the claim recite an additional element or a combination of elements, that when considered individually or in combination, "apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception." Guidance at 54.

A judicial exception is not integrated into a practical application when the claims are drawn to the mere use of "a computer as a tool to perform an abstract idea." Guidance, 84 Fed. Reg. at 55; *see Electric Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016) (finding that "the focus of the claims is not on . . . an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools"); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–6 (Fed. Cir. 2016) (determining whether the claims at issue were focused on a "specific asserted improvement in computer capabilities" or "a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool").

Here, we agree with Appellant that there is a practical integration of the abstract idea. In particular, we agree that "the claims of the present application describe a detailed process for improving the functioning of computer communications through the use of an authentication token and a resource request database" (App. Br. 13).

Enfish explains that "the first step in the Alice inquiry in this case asks whether the focus of the claims is on the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." *Enfish*,

822 F.3d at 1335–6. Applied to claim 26, we understand the claimed method to represent a technical improvement in a computer processing system rather than simply using the computer as a tool.

While this is a close case, the current claims do not simply use the computer and software as tools to perform a mental process and process of organizing human activity as routinely performed by a bank teller. Rather, as argued by Appellant, "the present claims involve storing transaction details in a database for later retrieval, and the creation, transfer, and verification of an authentication token to increase the security of computer communications to allow a secure transaction to be completed at a third hardware device." (App. Br. 14).

That is, the claims are drawn to methods of secure communication between two different computers, which is a problem uniquely faced by computer authentication systems and differs from the types of authentication problems faced by bank tellers and customers. Like *McRO* , that was drawn to a computer based process that improves operations on the computer animation process itself, claim 26 is intended to improve the authentication process of secure transactions on the security of the computer and ATM themselves. *See McRO, Inc. v. Bandai Namco Games Am. Inc*., 837 F.3d 1299 (Fed. Cir. 2016).

DDR held claims were directed to statutory subject matter because they claim a solution "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR Holdings, LLC v. Hotels.com, L.P*., 773 F.3d 1245, 1257 (Fed. Cir. 2014). The same reasoning applies here, because the authentication token problem for hardware and server devices arises in the realm of computer

networks, and differs from the authentication problems faced by bank tellers and customers.

Therefore, on this record, we conclude that the ineligible subject matter in Appellant's claim 26 is integrated into a practical application.

C. Guidance Step 2B

Having determined that the judicial exception is integrated into a practical application, we need not address whether claim 26 is well-understood, routine, conventional in the field, or simply appends well-understood, routine, conventional activities previously known to the industry. *See* 84 Fed. Reg. 51.

The rejection of the claims under 35 U.S.C. § 101 is reversed.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Basis	Affirmed	Reversed
26–35	112(b)			26–35
26–35	103	Labrou	26–35	
26–35	101			26–35
Overall Outcome			26–35	

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