UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/341,776	07/26/2014	Ezio Anselmo MAZARIM FERNANDES	PW-140103	2212

23662	7590	03/24/2020

ROBERT M. MCDERMOTT, ESQ.
1824 FEDERAL FARM ROAD
MONTROSS, VA 22520

EXAMINER
GETACHEW, WODAJO

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/24/2020	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):

claudia@artlover.com
patents@lawyer.com

UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD
_____

Ex parte ENZIO ANSELMO MAZARIM FERNANDES
_____

Appeal 2019-004538
Application 14/341,776
Technology Center 3600
_____

Before DONALD E. ADAMS, ERIC B. GRIMES, and
RICHARD M. LEBOVITZ, *Administrative Patent Judges*.

LEBOVITZ, *Administrative Patent Judge*.

DECISION ON APPEAL

The Examiner rejected the claims under 35 U.S.C. § 112(a) as lacking a written description, under 35 U.S.C. § 112(b) as indefinite, under 35 U.S.C. § 102 as anticipated, and under 35 U.S.C. § 103 as obvious. Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject the claims. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[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 PayWithMyBank, Inc. Appeal Br. 2.

STATEMENT OF THE CASE

The claims stand rejected by the Examiner as follows:

Claims 33–35 under 35 U.S.C. § 112(a) as failing to comply with the written description requirement. Final Act. 8.

Claims 33–35 under 35 U.S.C. § 112(b) as indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention. Final Act. 10.

Claims 33–35 under 35 U.S.C. § 102(a)(1) as anticipated by Shablygin et al. (US 2013/0145173 A1, published Jun. 6, 2013) ("Shablygin"). Final Act. 11.

Claims 33–35 under 35 U.S.C. § 103 as obvious in view of Shablygin, Kargman et al. (US 2008/0208697 A1, published Aug. 28, 2008) ("Kargman"), and Csoka (US2008/0109279 A1, published May 8, 2008) ("Csoka"). Ans. 13.

Claim 33, the only independent on review, is reproduced below (bracketed numbering added for reference to the limitations in the claim):

> 33. A non-transitory computer-readable medium that includes a program that, when executed by a processor system, causes the processor system to:
> during a first time interval:
> [1] receive sensitive information from a merchant system;
> [2] encrypt the sensitive information to form encrypted sensitive information;
> [3] use the sensitive information to provide an authentication of a purchaser's authorization to transfer the amount corresponding to the purchaser payment from an account associated with the purchaser to an account associated with the merchant system;
> [4] partition the encrypted sensitive information into a first encryption part and a second encryption part;

[5] create a token that identifies at least the first encryption part;

[6] store the first encryption part and a copy of the token;

[7] communicate the token, the second encryption part, and the authentication to the merchant system; and

[8] delete the second encryption part from the payment system; and

during a second time interval:

[9] receive the authorization, the token and the second encryption part from the merchant system;

[10] use the token to obtain the first encryption part;

[11] combine the first and second encryption parts to restore the encrypted sensitive information;

[12] decrypt the encrypted sensitive information to restore the sensitive information; and

[13] use the sensitive information to effect the transfer of the authorized payment from the account associated with the purchaser to the account associated with the merchant system.

WRITTEN DESCRIPTION REJECTION

The Examiner rejected claim 33 as failing to comply with the written description requirement, citing limitations [3], [7], [8], and [13] of the claim as a lacking a description in the Specification as originally filed. Final Act. 8, 9.

In responding to the rejection, Appellant did not identify support for the disputed limitations in the Specification. Instead, Appellant argues "that credit card payment processes and bank account transfer processes have been established for well over fifty years, and need not be detailed in a specification written in 2014" and the skilled worker "would know how to store and delete information from a system." Appeal Br. 12.

We address each limitation separately.

Limitation [3] uses "the sensitive information to provide an authentication of a purchaser's authorization to transfer the amount corresponding to the purchaser payment from an account associated with the purchaser to an account associated with the merchant system." The recited step of "authentication" does not appear in Figure 2 of the Specification, which illustrates an embodiment of the invention that includes steps of the claimed subject matter. Spec. ¶¶ 26, 31–40. The only reference to authentication in the Specification is a discussion of the recommendation not to store authentication data subsequent to authorization. Spec. ¶ 7. The issue is not whether the authentication step [3] is well-known, as asserted by Appellant, but rather whether the step is adequately described in the Specification to demonstrate that the inventor had possession of it in the claimed process. The Specification, as originally filed, must "convey[] with reasonable clarity to those skilled in the art that, as of the filing date sought, [that the inventor] was in possession of the invention." *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991). "One shows that one is 'in possession' of the invention by describing the invention, with all its claimed limitations." *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997). A description that merely renders the invention obvious does not satisfy the requirement. *Id.* at 1571–72. In this case, Appellant did not establish that one of ordinary skill in the art, upon reading the Specification would have understood it to describe the authentication step [3] of claim 33.

Appellant's argument addresses the obviousness of the step, but not how the step is described in Specification. "[I]t is the specification itself that must demonstrate possession. And while the description requirement does

not demand any particular form of disclosure, . . . or that the specification recite the claimed invention in haec verba, a description that merely renders the invention obvious does not satisfy the requirement." *Ariad Pharmaceuticals, Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1352 (Fed. Cir. 2010). We thus agree with the Examiner that Specification does not describe this step nor how it is implemented.

Limitation [7] recites "communicate the token, the second encryption part, and the authentication to the merchant system." Figure 2 of the Specification shows the TransactionID, Token, and Encrypted Piece2 communicated to the Merchant (110, 140, 232). Thus, the Specification describes communication of the token and second encryption part to the merchant, but not the "authentication" as required by the claim. Appellant did not guide us to where in the Specification this limitation is described. We thus agree with the Examiner that Specification does not describe this step nor how it is implemented.

Limitation [8] recites "delete the second encryption part from the payment system." Appellant did not identify where in the Specification this step is described. Figure 2 of the Specification does not show it. As explained above, Appellant's only argument is that payment processes were well known at the time of the invention, but Appellant did not identify where in the Specification the disputed limitation is described. Appeal Br. 12.

Limitation [13] recites "use the sensitive information to effect the transfer of the authorized payment from the account associated with the purchaser to the account associated with the merchant system." The Specification describes payment authorization as the last step when the

transaction is finalized. Spec. 15, 18, 25. Thus, we find this limitation described in the Specification.

The Examiner rejected the claims as lacking a written description, stating that the claim recited "functional language but does not describe how the function is performed" and referenced Manual of Patent Examining Procedure ("MPEP") § 2161.01 (Ninth Ed., Rev. Jan. 2018 [R-08.2017]). MPEP § 2161.01 states:

> When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter. Specifically, if one skilled in the art would know how to program the disclosed computer to perform the necessary steps described in the specification to achieve the claimed function and the inventor was in possession of that knowledge, the written description requirement would be satisfied. Hayes, 982 F.2d at 1534. If the specification does not provide a disclosure of the computer and algorithm in sufficient detail to demonstrate to one of ordinary skill in the art that the inventor possessed the invention including how to program the disclosed computer to perform the claimed function, a rejection under 35 U.S.C. 112, first paragraph for lack of written description should be made.

Appellant did not identify where in the Specification limitations [3], [7], and [8] are described, let alone the description of them in sufficient detail of how they are performed. Appellant's argument that such steps are well-established and enabled (Appeal Br. 11–12), does not adequately address the basis of the rejection.

For the foregoing reason, the rejection of claim 33, and dependent claims 34 and 35 which incorporate all the limitations of claim 33, is affirmed.

INDEFINITENESS REJECTION

The Examiner rejected claims 33–35 under § 112(b) because the claims recited "the amount," "the purchaser payment," and "the payment system" which lack antecedent basis for each of the terms. Final Act. 10.

As explained in MPEP § 2173.05(e):

> The lack of clarity could arise where a claim refers to "said lever" or "the lever," where the claim contains no earlier recitation or limitation of a lever and where it would be unclear as to what element the limitation was making reference . . . Obviously, however, the failure to provide explicit antecedent basis for terms does not always render a claim indefinite. If the scope of a claim would be reasonably ascertainable by those skilled in the art, then the claim is not indefinite.

In this case, there is no earlier recitation of amount, purchaser payment, or payment system. However, the term "the amount" is specifically defined in the claims as "the amount corresponding to the purchaser payment from an account associated with the purchaser to an account associated with the merchant system." Thus, we find this term to be definite because it is defined in the claim. The term "the purchaser payment" is also definite because, in view of its definition in the claim, the skilled worker would understand that it is "the payment" from the recited "account."

In step [8], the second encrypted part is deleted from "the payment system." We agree with the Examiner that "payment system" has no antecedent basis and is indefinite. The term is not defined in the claim. The recitation of "the payment system" implies there is "a payment system"

7

previously recited in the claim, but there is not. It is unclear whether "the payment system" is a part of "the merchant system" recited in the claim, or "a processor system" that is not necessarily part of the merchant system.

The Examiner also found that the claim is indefinite because it "is attempting to claim both an apparatus and the method steps of using the apparatus." Final Act. 11. We do not agree. The claim is a "non-transitory computer-readable medium" which is a "manufacture," one of the categories of inventions recited in 35 U.S.C. § 101. The manufacture comprises the program, which is recorded on the medium. However, the presence of the program on the "non-transitory computer-readable medium" does not make the claim indefinite because the medium's purpose is to carry an executable program and it does not change the nature of the manufacture because of what is recorded on it.

For the foregoing reasons, we affirm the rejection of claim 33 because the recitation of "the payment system" lacks antecedent basis and is therefore indefinite. Dependent claims 34 and 35 incorporate all the limitations of claim 33 and fall with claim 33 for the same reason.

ANTICIPATION REJECTION

The Examiner rejected claims 33–35 as anticipated by Shablygin. The Examiner did not give any weight to the executable program included on the recited "computer-readable medium." Final Act. 12. This determination is improper because the programmable instructions have a functional relationship with the computer. *See* MPEP 2111.05.III ("a claim to computer-readable medium programmed with attribute data objects that perform the function of facilitating retrieval, addition, and removal of information in the intended computer system, establishes a functional

8

relationship such that the claimed attribute data objects are given patentable weight."). The anticipation rejection of claims 33–35 is therefore reversed.

OBVIOUSNESS BASED ON SHABYLGIN, KARGMAN, AND CSOKA

The Examiner found that Shablygin describes steps [1]–[6] and [10]–[12] of claim 33. Final Act. 13–14.[2] The Examiner further found that Kargman describes [7] "communicate the token, the second encryption part" and [8] "delete the second encryption part from the payment system", and [9] "receive the authorization, . . . and the second encryption part from the merchant system." Final Act. 14–15. The Examiner found that Csoka describes step [13] of the claim. Final Act. 15.

In finding the claims obvious in view of Shablygin and Kargman, the Examiner explained:

> it would have been obvious to one of ordinary skill in the art to substitute the <u>data container identifier (token)</u>, the data container message sent to the merchant (Pars. 71, 195) and the delete operation request that the system destroy a data container (Par. 162) of Shablygin in view of Kargman in order to allow the merchant to retrieve customer profile using the token and make updates to the customer profile when completing transaction and store the updated profile securely (Shablygin, Par. 214) and to avoid compromising of the entire database impossible (Kargman, Par. 83). ("Express suggestion to substitute one equivalent technique for another need not be present to reader such substitution obvious"; *In re Fout,* 213 USPQ 532 (CCPA 1982), *In re Siebentritt,* 152 USPQ 618

---

[2] We note that certain of these steps are admitted to be prior art by Appellant as summarized in Figure 1 of the Specification, which when compared to Figure 2, shows the admitted differences between the disclosed invention and the prior art. It is not clear on the record before us whether the Examiner considered the admitted prior art of Figure 1 when making the rejection.

(CCPA 1967); *Ex Parte Smith,* 83 USPQ2d 1509 (Bd. Pat. App.
& Int. 2007); *KSR International Co. v. Teleflex Inc.,* 82
USPQ2d 1385 (U.S. 2007)).

Final Act. 15 (underlining added).

The Examiner's reason to combine Shablygin and Kargman is not
supported by a preponderance of the evidence. The "data container
identifier" described in Shablygin is generated from keys provided by the
user and the service provider. As explained in Shablygin:

> The data container 10 stores a data that a particular service
> provider is allowed to access, use and/or modify with the
> permission of the user. The data container 10 can be analogized
> to a virtual safe deposit box, where two keys are needed to open
> the virtual safe deposit box, with one key 22 belonging to the
> service provider and the other key 28 belonging to the user. To
> open the virtual safe deposit box (e.g., to access the data in the
> data container 10), both the user 26 and the service provider 20
> must provide their keys 28 and 22 which, when combined,
> generate *a unique data container identifier* 14 that enables
> access to the data stored in the data container 10. As such,
> because keys are needed from both the service provider 20 and
> the user 26 to determine the location of the data, access to the
> data stored in the data container 10 is restricted to the
> authorized user/service provider pair. *Requiring keys from both
> the service provider 20 and the user 26 additionally can
> provide the advantage of providing a system in which the
> storage provider 20 has no access to data except when the
> authenticated user 26 is present.*

Shablygin ¶ 71 (emphasis added).

Shablygin, as explained in paragraph 71, combines keys from the
service provider and the user to generate a "unique data container identifier"
that is used to open the data container that contains the sensitive and
encrypted data that the user seeks to protect (Shablygin ¶¶ 58, 61). The
purpose of the *data container identifier* is to block access to the data when

10

the authenticated user is not present. *Id.* at ¶ 71; ¶ 81 ("Since the A&DDS [authentication and dispersed data storage] system cannot create this encryption key without the presence of the authenticated user and of the authenticated service provider, during the absence of either party the stored data cannot be decrypted.") As discussed by Appellant (Appeal Br. 18–19), there would be no reason to communicate the data container identifier to the service provider (referred to as the "merchant" by the Examiner) because that would defeat the purpose of Shablygin which requires the presence of both the user and the service provider to ensure that the service provider does not have lone access to the data. The Examiner's reasoning that it would have been obvious to send the data container identifier to the merchant as a "token . . . in order to allow the merchant to retrieve customer profile using the token and make updates to the customer profile" would allow the merchant to have sole control of the user's sensitive information which is opposite to Shablygin's goal of protecting the user information from unilateral access by the service provider. Compare step [7] of claim 1: "communicate the *token*, the second encryption part, and the authentication to the merchant system."

Step [7] of claim 1 also requires that "the second encryption part" is sent to the merchant. The Examiner's determination that substituting the data container identifier for the token in Kargman as an "equivalent technique" is also not supported by a preponderance of the evidence. Kargman, as found by the Examiner, splits the credit card information into two pieces, and sends one piece to the merchant. Kargman ¶ 51. Shablygin's data container identifier does not contain encrypted data, itself. Therefore, sending the data

container identifier to the merchant is not the same as or equivalent to sending encrypted data to the merchant.

Accordingly, for the foregoing reasons, the rejection of claim 33 as obvious in view of Shablygin, Kargman, and Csoka is reversed. Dependent claims 34 and 35 incorporate all the limitations of claim 33 and are therefore reversed for the same reasons.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
33–35	112(a)	Written description	33–35	
33–35	112(b)	Indefiniteness	33–35	
33–35	102(a)(1)	Shablygin		33–35
33–35	103	Shablygin, Kargman, Csoka		33–35
Overall Outcome			33–35	

TIME PERIOD

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED