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.
15/169,260	05/31/2016	Oliver S. C. Quigley	SQR-10795-3;SQ-0032-US1C2	7468

129981	7590	10/17/2019

Mattingly & Malur, PC - Square
1800 Diagonal Road, Suite 210
Alexandria, VA 22314

EXAMINER
CHOO, JOHANN Y

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
10/17/2019	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):

cbarnitz@mmiplaw.com
ptomail@mmiplaw.com

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

———————

BEFORE THE PATENT TRIAL AND APPEAL BOARD

———————

Ex parte OLIVER S. C. QUIGLEY, NATHAN MCCAULEY, and
BOB LEE

———————

Appeal 2018-005781
Application 15/169,260
Technology Center 3600

———————

Before JOSEPH L. DIXON, JAMES W. DEJMEK, and
STEPHEN E. BELISLE, *Administrative Patent Judges.*

DIXON, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the

Examiner's decision to reject claims 1–6 and 22–34. Final Act. 1. Claims

7–21 were subject to a restriction requirement and have been canceled.

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(a) (2017). Appellant identifies the real party in interest as
Square, Inc. (App. Br. 1).

CLAIMED SUBJECT MATTER

The claims are directed to a software PIN entry. The Specification further discloses:

> The PIN can be entered on a touch display of the mobile computing device. This permits the mobile device to be a common consumer device, *e.g.,* an iPhone or iPad. When the card reader is attached to the mobile device, *e.g.,* plugged into the audio port, an application installed on the mobile computing device permits the mobile device to communicate with the card reader in order to process transactions.

(Spec. ¶ 6).

 Claim 28, reproduced below, is illustrative of the claimed subject matter:

> 28.   A method comprising:
>
> displaying on a display of a merchant device, by a merchant point-of-sale (POS) application, when executed by one or more processors of the merchant device, a user interface for entry of a personal identification number (PIN);
>
> receiving, by the merchant POS application, when executed by the one or more processors, input via the user interface, wherein the input represents a PIN;
>
> encrypting, by the merchant POS application, when executed by the one or more processors, the PIN using a copy of a first cryptographic key stored on the merchant device, wherein the first cryptographic key is a symmetric key shared between a card reader and the merchant POS application;
>
> transmitting, by the merchant POS application, when executed by the one or more processors, the encrypted PIN to the card reader;
>
> receiving, by the card reader, the encrypted PIN from the merchant device;
>
> decrypting, by the card reader, the encrypted PIN using a copy of the first cryptographic key stored on the card reader;

transmitting, by the card reader, the decrypted PIN to a card coupled to the card reader;

receiving, by the card reader, from the card, an approval of the PIN;

encrypting, by the card reader, using a second cryptographic key stored on the card reader, a message for the merchant device to generate an encrypted message for the merchant device;

transmitting, by the card reader, an encrypted message to the merchant device in response to receiving the approval of the PIN from the card;

receiving, by the merchant POS application, when executed by the one or more processors, the encrypted message from the card reader; and

transmitting, by the merchant POS application, when executed by the one or more processors, the encrypted message to a payment processing server.

REFERENCES

The prior art relied upon by the Examiner is:

Kageyama	US 2004/0096188 A1	May 20, 2004
Kohan et al.	US 2005/0256742 A1	Nov. 17, 2005
Adams et al.	US 2008/0017711 A1	Jan. 24, 2008
Tang et al.	US 2012/0061467 A1	Mar. 15, 2012
Quigley et al.	US 9,367,842 B2	June 14, 2016

(applied in the obviousness-type double patenting rejection)

REJECTIONS

Claims 1–6 stand rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1–6 and 9 of U.S. Patent No. 9,367,842 (Quigley).

Claims 1–6 and 22–34stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to patent-ineligible subject matter.

Claims 1, 2, 6, 22, 23, 27, 28, 29, 33, and 34 stand rejected under 35 U.S.C. § 103 as being unpatentable over Tang in view of Adams.

Claims 3, 24, and 30 stand rejected under 35 U.S.C. § 103 as being unpatentable over Tang in view of Adams as applied to claim 1 in further view of Kageyama.

Claims 4, 5, 25, 26, 31, and 32 stand rejected under 35 U.S.C. § 103 as being unpatentable over Tang in view of Adams as applied to claim 1 in further view of Kohan.

OPINION

Obviousness-Type Double Patenting

With respect to claims 1–6, the Examiner generally maintains that although the claims at issue are not identical, they are not patentably distinct from each other because the claims of the current application are obvious variations or are an obvious variation of a combination of the claims of Patent No. 9,367,842. (Final Act. 13). The Examiner also maintains that removing the "preventing" step from the patented claim 1 does not change the overall process of the current claims and the current claims recite very similar processes. (Ans. 9). The Examiner further maintains that:

> all of these processes are found in the current claims with merely obvious variations. Variations such as having the card authenticate the PIN and send a response is merely a combination of typical EMV processes, as already discussed above as being conventional, and forwarding such information to the merchant device, which already falls within the claimed step of receiving further information form the card reader and continuing communications.

(Ans. 9).

Appellant contends that the Examiner makes unsupported allegations and conclusions based on, e.g., the claims allegedly "recit[ing] similar

4

processes," and the Examiner has failed to provide any evidence to support the assertion that the differences between Appellant's claims 1–6 and the patented claims of are not patentably distinct. (App. Br. 14–15).

We agree with Appellant that the Examiner's rejection is based upon unsupported allegations where the Examiner has not provided evidence to support the Examiner's findings and obviousness conclusion. The Examiner has relied upon the claims of the prior patent and not provided any additional documentary evidence to support the Examiner's factual findings and obviousness conclusion. Also, the Examiner has rejected the claimed "system" of the present claims based upon the "method" claims 1–6 and an additional "system" in dependent claim 9 of the 9,367,842 patent where all the limitations of the claims of the 9,367,842 patent are directed to process limitations at the mobile device rather than the combination of a mobile device and card reader as recited in the rejected claim 1.

Furthermore, the Examiner maintains "[v]ariations such as having the card authenticate the PIN and send a response is *merely a combination of typical EMV processes*, as already discussed above as being conventional." (Ans. 9) (emphasis added). The Examiner has not provided or relied upon any additional teachings or disclosures to support the Examiner's proffered obvious modifications of the claims of the 9,367,842 patent.[2] Additionally,

---

[2] We leave it to the Examiner to further consider prior art of record in the 9,367,842 patent in consideration of any further obviousness-type double patenting rejection or obviousness rejection. For example, "A Guide to EMV-Version 1.0," EMVCo LLC, dated May 2011, pp. 1–35; "MasterCard PayPass, Terminal Implementation Requirements," Mastercard Worldwide, 2007 v. 1, dated Sept. 10, 2015, pp. 1–62; and Fillmore, P., "Mobile and Contactless Payment and Security," v20111118, Witham Laboratories, dated Nov. 18, 2011, pp. 1–39. (Filed in an IDS on December 14, 2015 in the

the Examiner has not identified any specific correlation between any of the rejected dependent claims and the patented claims. As a result, we do not sustain the nonstatutory obviousness-type double patenting rejection of claims 1–6.

35 U.S.C. § 101

With respect to the patent eligibility rejection of independent claims 1, 22, and 28, Appellant argues the claims together and addresses independent claim 1. We select independent claim 28 as the representative claim for the group because it more clearly shows the sequence of steps in order within the claimed process and will address Appellant's arguments thereto. *See* 37 CFR 41.37 (c)(1)(iv).

Appellant disputes the Examiner's conclusion that the pending claims are directed to patent-ineligible subject matter. (App. Br. 33–48; Reply Br. 5–13). Appellant's general contention is that the Examiner's

> characterization discounts the scope and character of Appellant's claims. Appellant respectfully submits that the Examiner has failed to consider the claims as a whole and, in the above analysis, has cherry picked some elements of Appellant's claims to support the Examiner's position, while completely ignoring other specific elements of Appellant's claims that clearly direct Appellant's claims to an improvement in the function of a computing system.

(App. Br. 37; Reply Br. 7–8). Appellant further contends that:

> in the discussion of the rejections under 35 U.S.C. § 103, none of these elements are taught or suggested by the prior art. Thus, Appellant's claim provides a non-conventional and non-generic

---

prosecution history of patent 9,367,842 and filed in an IDS in this application on June 15, 2016).

> system and method for protecting a PIN from being capture by a
> malicious actor, which improves the security of the system and
> thereby provides a technical solution to a technical problem
> rooted in computer technology. As stated in *Enfish,* "[s]oftware
> can make non-abstract improvements to computer technology
> just as hardware improvements can." *See Enfish,* 822 F.3d at
> 1339.[3] Abstraction is avoided or overcome when a proposed
> new application or computer-implemented function is not simply
> the generalized use of a computer as a tool to conduct a known
> or obvious process, but instead is an improvement to the
> capability of the system as a whole. *Id.* at 1336.

(App. Br. 37; *see generally* Reply Br. 8–11). Appellant also contends that

"[t]he claimed invention is directed to an improvement in the security of

communications between a card reader, a mobile device, a payment card,

and a server when performing a payment transaction, and thereby improves

the security of the devices themselves and the data thereon." (App. Br. 38;

see generally Reply Br. 11). Appellant argues that the claimed invention:

> pertains to electronically encrypting and decrypting sensitive
> information transmitted between a computing device, a card
> reader, and a payment card during a transaction using encryption
> of a personal identification number (PIN) to protect the PIN from
> exposure to malware or other malicious code. Without the
> techniques described in Appellant's claims, the PIN may be
> stolen or otherwise compromised. Thus, Appellant's Claim 1
> includes an improvement in the security function of the
> computing device and the card reader.

(App. Br. 38; *see generally* Reply Br. 11). We find Appellant's arguments

unpersuasive.

The Supreme Court's two-step framework guides our analysis of

patent eligibility under 35 U.S.C. § 101. *Alice Corp. v. CLS Bank Int'l*, 573

U.S. 208, 217 (2014). In addition, the Office recently published revised

---

[3] *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016)

guidance for evaluating subject matter eligibility under 35 U.S.C. § 101, specifically with respect to applying the *Alice* framework. USPTO, *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019) ("Office Guidance"). If a claim falls within one of the statutory categories of patent eligibility (i.e., a process, machine, manufacture, or composition of matter) then the first inquiry is whether the claim is directed to one of the judicially recognized exceptions (i.e., a law of nature, a natural phenomenon, or an abstract idea). *Alice*, 573 U.S. at 217. As part of this inquiry, we must "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 Tex., LLC v. DirecTV, LLC*, 838 F.3d 1253, 1257–58 (Fed. Cir. 2016) (internal citations omitted). Per Office Guidance, this first inquiry has two prongs of analysis (i) does the claim recite a judicial exception (e.g., an abstract idea), and (ii) if so, is the judicial exception integrated into a practical application. 84 Fed. Reg. at 54. Under the Office Guidance, if the judicial exception is integrated into a practical application, *see infra*, the claim passes muster under § 101. 84 Fed. Reg. at 54–55. If the claim is directed to a judicial exception (i.e., recites a judicial exception and does not integrate the exception into a practical application), the next step is to determine whether any element, or combination of elements, amounts to significantly more than the judicial exception. *Alice*, 573 U.S. at 217; 84 Fed. Reg. at 56.

Step 2A, Prong One

For the reasons discussed below, we conclude Appellant's claim 28 recites an abstract idea. Appellant's claims generally recite a "method" comprising: i) encrypting the PIN; ii) decrypting, by the card reader, the

encrypted PIN using a copy of the first cryptographic key stored on the card

reader; iii) encrypting, by the card reader, using a second cryptographic key

stored on the card reader, a message for the merchant device to generate an

encrypted message for the merchant device.[4] This is consistent with how

Appellant describes the claimed embodiment of the invention. (*See, e.g.*,

description of Figures 3–6, 9–11; Spec. ¶¶ 3, 29, 30, 46, 49, 55, 56, 59, 60,

64, 77–81, 86). (*See* App. Br. 6–7 Summary of the Claimed Subject Matter).

> The Examiner maintains that:

> all of these limitations amount to merely sending/receiving
> transaction data in a process that is utilized in smartcard financial
> processes in a conventional manner with the added use of
> encryption, which is also conventional for financial transactions.
> That is, the claims are directed to managing financial data in
> order to process a transactions, and this process is performed as
> just a combination of abstract ideas, e.g. processing information
> through a clearinghouse, comparing old and new data,
> transforming one form of data to another, etc. such a combination
> of abstract ideas does not cause the claims to overcome the
> individual abstract ideas, as the combination of abstract ideas is
> still abstract.

(Ans. 6).

Moreover, the Federal Circuit holds that claims broadly covering data

collection, communication, and processing are directed to abstract ideas.

See, *e.g.*, *Univ. of Fla. Research Found., Inc. v. Gen. Elec. Co.*, 916

F.3d 1363, 1366–68 (Fed. Cir. 2019); *SAP Am., Inc. v. InvestPic LLC*, 898

---

[4] We further note that the language of independent claim 28 does not
expressly recite any of the additional processing performed at any of the
hardware devices beyond the encrypting and decrypting steps and the
receiving and transmitting steps.

F.3d 1161, 1164–67 (Fed. Cir. 2018); *Secured Mail Sols. LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 907–08, 910–11 (Fed. Cir. 2017); *Credit Acceptance Corp. v. Westlake Services,* 859 F.3d 1044, 1055, 123 USPQ2d 1100, 1108-09 (Fed. Cir. 2017); *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1326–27 (Fed. Cir. 2017); *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1339–41 (Fed. Cir. 2017). As the Federal Circuit has explained, "[a] process that start[s] with data, add[s] an algorithm, and end[s] with a new form of data [is] directed to an abstract idea." *RecogniCorp*, 855 F.3d at 1327.

Claim 28 is reproduced below and includes the following claim limitations, emphasized in *italics,* which recite a generic method encrypting the PIN, decrypting the encrypted PIN and encrypting a message:

> A method comprising:
> displaying on a display of a merchant device, by a merchant point-of-sale (POS) application, when executed by one or more processors of the merchant device, a user interface for entry of a personal identification number (PIN);
> receiving, by the merchant POS application, when executed by the one or more processors, input via the user interface, wherein the input represents a PIN;
> *encrypting,* by the merchant POS application, when executed by the one or more processors, *the PIN using a copy of a first cryptographic key stored on the merchant device, wherein the first cryptographic key is a symmetric key shared between a card reader and the merchant POS application*;
> transmitting, by the merchant POS application, when executed by the one or more processors, the encrypted PIN to the card reader;
> receiving, by the card reader, the encrypted PIN from the merchant device;
> *decrypting,* by the card reader, *the encrypted PIN using a copy of the first cryptographic key stored on the card reader*;

> transmitting, by the card reader, the decrypted PIN to a card coupled to the card reader;
>
> receiving, by the card reader, from the card, an approval of the PIN;
>
> *encrypting*, by the card reader, using a second cryptographic key stored on the card reader, *a message for the merchant device to generate an encrypted message for the merchant device*;
>
> transmitting, by the card reader, an encrypted message to the merchant device in response to receiving the approval of the PIN from the card;
>
> receiving, by the merchant POS application, when executed by the one or more processors, the encrypted message from the card reader; and
>
> transmitting, by the merchant POS application, when executed by the one or more processors, the encrypted message to a payment processing server.

More particularly, the generic method of encrypting the PIN, decrypting the encrypted PIN, and encrypting a message is a mathematical concept and consistent with our Office Guidance and case law, we conclude that encrypting the PIN, decrypting the encrypted PIN and encrypting a message is a mathematical concept and, thus, an abstract idea.[5] *See* 84 Fed. Reg. at 52.

---

[5] Our reviewing court recognizes that "[a]n abstract idea can generally be described at different levels of abstraction." *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1240 (Fed. Cir. 2016). That need not and, in this case does not, "impact the patentability analysis." *Id.* at 1241. Further, "[a]n abstract idea can generally be described at different levels of abstraction . . . . The Board's slight revision of its abstract idea analysis does not impact the patentability analysis." *Id.* Moreover, merely combining several abstract ideas does not render the combination any less abstract. *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) ("Adding one abstract idea (math) to another abstract idea . . . does not render the claim non-abstract."); *see also FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d

11

Step 2A, Prong Two

Because the claim recites an abstract idea, we next determine whether

the claim integrates the abstract idea into a practical application. 84 Fed.

Reg. at 54. To determine whether the judicial exception is integrated into a

practical application, we identify whether there are "*any additional elements*

recited in the claim beyond the judicial exception(s)" and evaluate those

elements to determine whether they integrate the judicial exception into a

recognized practical application. 84 Fed. Reg. at 54–55 (emphasis added);

1089, 1093–94 (Fed. Cir. 2016) (determining the pending claims were
directed to a combination of abstract ideas).

Thus, the patentability analysis in this Appeal does not turn on exactly
how various limitations are characterized as being abstract, i.e., as either an
abstract "mathematical concept," "mental process," or "certain methods of
organizing human activity." For example, the decrypting and encrypting
limitations can alternatively be characterized as mathematical concepts
claimed at a high level, and can be characterized as reciting mental
processes. The end result remains the same in this Appeal. The claim
recites an abstract idea.

See also, SAP America, Inc. v. *InvestPic, LLC*, 898 F.3d 1161, 1163
(Fed. Cir. 2018) (holding that claims to a ''series of mathematical
calculations based on selected information'' are directed to abstract ideas);
Digitech Image Techs., LLC v. *Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1350
(Fed. Cir. 2014) (holding that claims to a ''process of organizing
information through mathematical correlations'' are directed to an abstract
idea); *Bancorp Servs., LLC* v. *Sun Life Assurance Co. of Can. (U.S.)*, 687
F.3d 1266, 1280 (Fed. Cir. 2012) (identifying the concept of ''managing a
stable value protected life insurance policy by performing calculations and
manipulating the results'' as an abstract idea).

see also Manual of Patent Examining Procedure ("MPEP") § 2106.05(a)–
(c), (e)–(h) (9th ed., Rev. 08.2017, Jan. 2018).

Here, we find the additional limitation(s) do not integrate the judicial
exception into a practical application. More particularly, the claims do not
recite (i) an improvement to the functionality of a computer or other
technology or technical field (*see* MPEP § 2106.05(a)); (ii) a "particular
machine" to apply or use the judicial exception (*see* MPEP § 2106.05(b));
(iii) a particular transformation of an article to a different thing or state
(*see* MPEP § 2106.05(c)); or (iv) any other meaningful limitation
(*see* MPEP § 2106.05(e)). *See* 84 Fed. Reg. at 55.

Rather, the steps of "displaying on a display of a merchant device, by
a merchant point-of-sale (POS) application, when executed by one or more
processors of the merchant device, a user interface for entry of a personal
identification number (PIN)," "receiving, by the merchant POS application,
when executed by the one or more processors, input via the user interface,
wherein the input represents a PIN," "transmitting," and "receiving" indicate
such activity is the type of extra-solution activities (i.e., in addition to the
judicial exception) the courts have determined insufficient to transform
judicially excepted subject matter into a patent-eligible application. *See*
MPEP § 2106.05(g); *see Electric Power Group, LLC v. Alstom S.A.*, 830
F.3d 1350 (Fed. Cir. 2016) (explaining that "selecting information, by
content or source, for collection analysis, and display does nothing
significant to differentiate a process from ordinary mental processes"); *Elec.
Power*, 830 F.3d at 1354 (recognizing "that merely presenting the results of
abstract processes of collecting and analyzing information, without more
(such as identifying a particular tool for presentation), is abstract as an
ancillary part of such collection and analysis"); *Bancorp Servs., L.L.C. v.*

Sun Life Assur. Co. of Can., 771 F.Supp.2d 1054, 1065 (E.D. Mo. 2011) *aff'd*, 687 F.3d 1266 (Fed. Cir. 2012) (explaining that "storing, retrieving, and providing data . . . are inconsequential data gathering and insignificant post solution activity").

Contrary to Appellant's arguments (*see, e.g.*, Reply Br. 7–8), the claims are not directed to a technological improvement or improvement in the function of a computing system. Although Appellant characterizes the claimed invention as "a nonconventional and non-generic system and method for protecting a PIN from being capture[d] by a malicious actor, which improves the security of the system and thereby provides a technical solution to a technical problem rooted in computer technology," Appellant does not identify the technological "problem" being solved, but merely uses conventional encryption in its usual manner. (*See* Reply Br. 8). The purported improvement, however, relates to the abstract idea, and does not improve a computer, technology, or a technical field. *See McRO, Inc. v. Bandai Namco Games America, Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) ("We . . . look to whether the claims in these patents focus on a specific means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery.") (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016)). Further, Appellant does not explain how the "method [for protecting a PIN]" recited in claim 28, for example, is not merely the routine or conventional use of the encryption and decryption (mathematical processing). *See DDR Holdings*, 773 F.3d at 1258–59 ("We caution, however, that not all claims purporting to address Internet-centric challenges are eligible for patent.").

Here, Appellant's claims do not recite specific limitations (or a combination of limitations) that are not generic. Receiving or sending information (e.g., the steps of "displaying on a display of a merchant device, by a merchant point-of-sale (POS) application, when executed by one or more processors of the merchant device, a user interface for entry of a personal identification number (PIN)," "receiving, by the merchant POS application, when executed by the one or more processors, input via the user interface, wherein the input represents a PIN," "transmitting," and "receiving") merely requires the well understood function of a computer/computer network. *See buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) ("That a computer receives and sends the information over a network—with no further specification—is not even arguably inventive."). In addition, we note Appellant describes the components of the claimed invention at a high level of generality and the components perform generic functions that are well-understood, routine, and conventional. (*See e.g.*, Spec. ¶¶ 87–96).

We further note that the Specification throughout discloses the use of encrypting and decrypting data, but provides no corresponding disclosure beyond "symmetric" and "asymmetric" encryption. (*See generally* Spec. ¶¶ 8, 50, 74, 80, and 82).

Moreover, Appellant's Specification discloses "[p]rocessors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer." (*See* Spec. ¶ 92). Additionally, the claims do not address a problem necessarily rooted in computer technology or a problem in the software arts. (*See* App. Br. 38–42; *see also* MPEP § 2106.05(a)).

15

Here, unlike the claims at issue in *DDR Holdings* Appellant's claims do not address a specific problem arising in the realm of computer networks (i.e., encrypting and decrypting data does not arise in the realm of computer networks where the encrypting and decrypting of data is not detailed in the claims), nor do they improve an existing technological process, but rather merely use computers and computer devices that operate in their normal, expected manner. *See DDR Holdings*, 773 F.3d at 1258–59; *see also Enfish*, 822 F.3d at 1335–36 (distinguishing between claims *wherein the focus of the claims* is on an improvement in computer capabilities and those that invoke a computer as a tool).

Here, Appellant's claim 28 merely generally links the use of a judicial exception to a particular technological environment. That is, although Appellant's claims recite hardware components (generic processors, display, merchant device, user interface, card reader, and payment processing server) the processors and other computer related devices, are configured to perform functions a computer would normally be expected to perform, adding nothing of substance to the underlying abstract idea. Thus, the claims' limitations are not indicative of "integration into a practical application." Rather, the processors and computer devices are readily available computing elements using their already available basic functions as tools in executing the claimed process steps. *See SAP Am., Inc. v. InvestPic LLC*, 898 F.3d 1161 (Fed. Cir. 2018).

For at least the foregoing reasons, the claims do not integrate the judicial exception into a practical application.

Step 2B

Because we determine the claims are directed to an abstract idea or combination of abstract ideas, we analyze the claims under step two of *Alice* to determine if there are additional limitations that individually, or as an ordered combination, ensure the claims amount to "significantly more" than the abstract idea. *Alice*, 573 U.S. at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72–73, 77–79 (2012)). As stated in the Office Guidance, many of the considerations to determine whether the claims amount to "significantly more" under step two of the *Alice* framework are already considered as part of determining whether the judicial exception has been integrated into a practical application. 84 Fed. Reg. at 56. Thus, at this point of our analysis, we determine if the claims add a specific limitation, or combination of limitations, that is not well-understood, routine, conventional activity in the field, or simply appends well-understood, routine, conventional activities at a high level of generality. 84 Fed. Reg. at 56.

Here, Appellant's claims do not recite specific limitations (or a combination of limitations) that are not well-understood, routine, and conventional. As discussed above, sending or receiving information (e.g., the steps of "displaying on a display of a merchant device, by a merchant point-of-sale (POS) application, when executed by one or more processors of the merchant device, a user interface for entry of a personal identification number (PIN)," "receiving, by the merchant POS application, when executed by the one or more processors, input via the user interface, wherein the input represents a PIN," "transmitting," and "receiving") merely requires the well-understood function of a computer/computer network. *See buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) ("That

17

a computer receives and sends the information over a network—with no

further specification—is not even arguably inventive."). Moreover,

Appellant's recitation of the claim limitations and conclusory statement that

the features amount to *"significantly more"* than just an abstract idea

(*see* App. Br. 43–48) is not supported by persuasive evidence or reasoning.

It is well settled that mere attorney arguments and conclusory statements,

which are unsupported by factual evidence, are entitled to little probative

value. *In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997); *see also In re*

Pearson, 494 F.2d 1399, 1405 (CCPA 1974) (attorney argument is not

evidence).

Because the Specification describes the additional element in general

terms, without describing the particulars, we conclude the claim limitation

may be broadly but reasonably construed as reciting conventional computer

components and techniques, particularly in light of Appellant's

Specification, as discussed above.[6]

Additionally, to the extent Appellant contends the claims do not seek

to tie-up (i.e., preempt) an abstract idea (*see* App. Br. 48; Reply Br. 13), we

are unpersuaded of Examiner error. "'[W]hile preemption may signal patent

ineligible subject matter, the absence of complete preemption does not

demonstrate patent eligibility.'" *FairWarning IP*, 839 F.3d at 1098 (Fed.

Cir. 2016) (quoting *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d

1371, 1379 (Fed. Cir. 2015)); *see also OIP Techs., Inc. v. Amazon.com, Inc.*,

788 F.3d 1359, 1362–63 (Fed. Cir. 2015) ("[T]hat the claims do not preempt

---

[6] Claim terms are to be given their broadest reasonable interpretation, as
understood by those of ordinary skill in the art and taking into account
whatever enlightenment may be had from the Specification. *In re Morris*,
127 F.3d 1048, 1054 (Fed. Cir. 1997).

all price optimization or may be limited to price optimization in the e-commerce setting do not make them any less abstract."). Further, "[w]here a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, as they are in this case, preemption concerns are fully addressed and made moot." *Ariosa*, 788 F.3d at 1379.

For the reasons discussed *supra*, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner's rejection of claims 1– 6 and 22–34 under 35 U.S.C. § 101. *See* 37 CFR. § 41.37(c)(1)(iv).

35 U.S.C. § 103

With respect to independent claims 1, 22, and 28, we address independent claim 1 as the illustrative claim for the group because it correlates with Appellant's arguments, and we address Appellant's arguments thereto.

With respect to illustrative claim 1, Appellant contends that the Examiner has provided mere conclusory statements in an attempt to meet the recitations of independent claim 1, but has not provided any objectively verifiable evidence in support of the interpretation. (App. Br. 10). Appellant further contends that "the Office has failed to cite any reference that teaches or suggests a card reader that decrypts an encrypted PIN, let alone a card reader that receives the encrypted PIN from a merchant device and decrypts the encrypted PIN using a copy of a first cryptographic key stored on the card reader." (App. Br. 12; Reply Br. 2–3).

The Examiner merely identifies that the MCU in the Tang reference is used to convert data that is originally in an encrypted format, and it would have been received in an encrypted format. (Ans. 3–4). We agree with the

Appellant that the Examiner has not shown that the card reader in the Tang reference decrypts the PIN data or suggests decrypting the PIN data.

Additionally, Appellant contends that the Examiner fails to cite any portion of the Tang or Adams references that teaches or suggests at least "the card reader configured to ... transmit the PIN to a card coupled to the card reader, [and] receive an approval of the PIN from the card." (App. Br. 18–19). Appellant further contends that "there are numerous different types of EMV standards used by these companies, and these standards are periodically being updated and changed. Appellant also contends that the Examiner has failed to point to any particular EMV standard or any other documentary evidence that actually teaches what the Examiner asserts to be a conventional process." (Reply Br. 5).

We agree with Appellant that the Examiner has not specifically provided any documentary evidence to support the Examiner's findings or conclusion of obviousness.

Appellant argues that the Examiner has failed to cite any portion of the Tang or Adams references that teaches or suggests at least "the card reader configured to ... encrypt a message for the merchant device using a second cryptographic key stored on the card reader to generate the encrypted message, and transmit the encrypted message to the merchant device in response to receiving the approval." (App. Br. 21–22) (emphasis omitted). Appellant also argues that the Tang reference merely describes a card reader that receives a PIN via a keypad and sends the PIN to a device, and the Examiner has failed to cite any document that teaches or suggests a merchant device that sends a PIN to a card reader. Appellant further argues that the Adams reference does not teach a merchant device and card taught by Adams is not an EMV card and does not use EMV standards. Therefore,

20

Appellant argues that the Examiner is making mere conclusions with any

supporting documentary evidence. (Reply Br. 6).

 We agree with Appellant that the Examiner has not specifically

provided any documentary evidence to support the Examiner's findings or

conclusion of obviousness.[7]

 Here, the Examiner's obviousness rejection is not well supported by

the express disclosures of the Tang and Adams references. Accordingly, we

agree with Appellant the Examiner's determination that the claimed

invention would have been obvious to a person of ordinary skill in the art is

in error because it is not supported by a preponderance of the evidence. *See*

In re Caveney, 761 F.2d 671, 674 (Fed. Cir. 1985) (Examiner's burden of

proving non-patentability is by a preponderance of the evidence); *see also In*

re Warner, 379 F.2d 1011, 1017 (CCPA 1967) ("The Patent Office has the

initial duty of supplying the factual basis for its rejection. It may not,

because it may doubt that the invention is patentable, resort to speculation,

unfounded assumptions or hindsight reconstruction to supply deficiencies in

its factual basis."). We will not resort to such speculation or assumptions to

cure the deficiencies in the factual basis in order to support the Examiner's

obviousness rejection. Consequently, we reverse the obviousness rejection

of illustrative independent claim 1 and its dependent claims 2 and 6 based on

---

[7] We note that the Examiner has identified paragraphs 104 and 105 of the
Tang reference which generally identify sending and receiving cash
payments with the use of a card reader and a cell phone, but the Tang
reference merely identifies "encoding" and "decoding" rather than
"encrypting" and "decrypting" these financial transactions. We leave it to
the Examiner to further consider the additional prior art references identified
above with respect to the obviousness-type double patenting rejection.

obviousness.[8] Independent claims 22 and 28 contain similar process limitations as independent claim 1. As a result, we reverse the obviousness rejection of claims 22 and 28 and their respective dependent claims 23, 27, 29, 33, and 34 based upon the noted deficiency in the Examiner's obviousness rejection.

With respect to dependent claims 3–5, 24–26, and 30–32, the Examiner has not identified how the additional prior art references remedy the deficiency in the obviousness rejection as noted above, and we cannot sustain the obviousness rejection of these claims for the same reason.

DECISION

We reverse the Examiner's obviousness-type double patenting and obviousness rejections, but we affirm the Examiner's patent-ineligible subject matter rejection.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Basis	Affirmed	Reversed
1–6		Nonstatutory obviousness-type double patenting		1–6
1–6 and 22–34	101		1–6, 22–34	

---

[8] We do not opine herein on whether the steps identified by the Examiner would have been obvious based upon the proffered unsupported statements, but find that the Examiner has not provided documentary evidence to support this conclusion. We leave it to the Examiner to further consider this issue in any further prosecution on the merits. Although the Board is authorized to reject claims under 37 C.F.R. § 41.50(b), no inference should be drawn when the Board elects not to do so. *See* MPEP § 1213.02.

Claims Rejected	35 U.S.C. §	Basis	Affirmed	Reversed
1, 2, 6, 22, 23, 27, 28, 29, 33, 34	103	Tang and Adams		1, 2, 6, 22, 23, 27–29, 33, 34
3–5, 24–26, 30–32	103	Tang and Adams in view of Kageyama or Kohan		3–5, 24–26, 30–32
Overall outcome			1–6, 22–34	

FINALITY AND RESPONSE

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

AFFIRMED