Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: PHILLIPS et al.	Confirmation No.: 8558
Application Serial No.: 15/637,747	Group Art Unit: 3695
Filing Date: June 29, 2017	Examiner: Benjamin S. Brindley
For: DATA SHARING WITH CARD ISSUER VIA WALLET APP IN PAYMENT-ENABLED MOBILE DEVICE	**APPEAL BRIEF** Docket No.: P03672-US-UTIL (M01.475) **PTO Customer Number 125619** Buckley, Maschoff & Talwalkar LLC 50 Locust Avenue New Canaan, CT 06840

CERTIFICATE OF ELECTRONIC TRANSMITTAL

The undersigned hereby certifies that this correspondence is being electronically submitted via EFS-Web on the date given below.

Dated of Transmittal: November 6, 2024

By: / Claire Murray /
Claire Murray

MS Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellant hereby appeals to the Board of Patent Appeals and Interferences from the Decision of the Examiner in the Final Office Action mailed May 10, 2024 (the "Final Action" hereinafter), and from the Panel Decision mailed on October 1, 2024, which directs Applicant to proceed to the Patent Trial and Appeal Board.

REAL PARTY IN INTEREST

The present application is assigned to MASTERCARD INTERNATIONAL INCORPORATED, 2000 Purchase Street, Purchase, New York 10577, U.S.A.

RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known to Appellant, Appellant's legal representative, or assignee, which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1, 4-10, 13, 14, 16 and 18 are pending in this application.

The pending claims stand rejected solely under Section 101 as allegedly being directed to non-statutory subject matter.

Claims 1, 4-10, 13, 14, 16 and 18 are now being appealed.

STATUS OF AMENDMENTS

Appellant filed an Amendment After Final Action on August 21, 2024 which addressed a Section 112(b) rejection[1] presented in the Final Action. In particular, minor amendments were made to independent claims 1, 14 and 16 and to dependent claims 4-6, 8-10 and 18. The amendments required only a cursory review by the Examiner and placed the claims in better form for consideration on appeal. Specifically, verbiage deemed unclear in the independent claims was canceled in order to overcome the Section 112(b) rejections, and the term "smartphone processor" was included in the independent and dependent claims (where necessary) for the sake of clarity and consistency. No new matter was added, and the Examiner entered the amendments prior to the filing of a Pre-Appeal Brief Request for Review.

[1] See Final Action, page items 3-4 on pages 2-3.

SUMMARY OF CLAIMED SUBJECT MATTER

At the time the invention was made the inventors recognized that opportunities existed to enhance the capability to detect and prevent fraud in situations wherein a smartphone running a merchant wallet application is utilized to conduct a payment transaction.[2] Thus, the claimed process includes a smartphone processor running a merchant wallet application to receive, via an NFC component from a merchant's POS terminal, an electronic receipt; generate transaction detail data including product item identification and a respective price range for each product item; and then transmit the transaction detail data to a transaction authentication server without revealing the exact price of any product item. Such functionality permits the transaction authentication server to use the transaction detail data to conduct risk management processing, and thus the process also includes the smartphone processor receiving a response message from the transaction authentication server indicating transaction authentication. The smartphone processor than transmits payment credential information stored in a storage device of the smartphone to at least one of the merchant POS and a payment processor.[3]

The claimed processes solve the technological problem of how to provide transaction detail data, including a useful indication of item pricing, to an authentication server without revealing the exact price of any product item, so that the authentication server can then utilize the transaction detail to apply reliable and sophisticated risk management algorithms to the transaction which involves a smartphone and a merchant POS terminal.[4] These goals are achieved by having the smartphone processor running the merchant wallet application generate and then transmit transaction detail data via the internet to the transaction authentication server without revealing the exact price of any product item so that risk management processing can be conducted before the smartphone processor receives a response message.[5] The process thus advantageously provides added assurance to an issuer that the transaction is legitimate in a manner that is transparent to the user, and which beneficially allows the payment transaction to proceed according to terms that are favorable to the merchant (concerning factors such as

[2] See published U.S. application (US 2018/0032996) at paragraphs 0011 and 0062.
[3] See claim 1.
[4] Published U.S. application (US 2018/0032996) at paragraphs 0060 and 0062.
[5] *Id.* at paragraph 0062.

interchange and/or shifting of liability to the issuer) in case the transaction ultimately proves to be problematic.[6]

* * * * * * *

Appellant will now map independent claims 1, 10 and 16 to the disclosure of the present application. All references to the application herein are to page and line numbers of the patent application as filed.

[6] *Id.* at paragraph 0018.

Claim 1

"A method of operating a smartphone running a merchant wallet application to enhance the capability for detecting and preventing fraudulent purchase transactions, the wallet application issued by a merchant, the method comprising:" – Specification on page 4, lines 3-6; on page 11, lines 30-34; and in FIG. 5.

"Receiving, by a processor of the smartphone running the merchant wallet application via a near-field communication (NFC) component from a merchant point of sale (POS) terminal, an electronic receipt including data identifying purchased items and a price per item" –Specification on page 7, lines 8-15 ; on page 9, lines 9-14; and in FIGS. 2, 3 and 5.

"Generating, by the smartphone processor running the merchant wallet application based on the data of the electronic receipt, transaction detail data comprising identification data of each product item being purchased and respective price range data for each identified product item" --Specification on page 10, lines 32 to page 11, line 1; on page 11, lines 5-9; and in FIG. 5.

"Transmitting, by the smartphone processor, the transaction detail data via the internet from the merchant wallet application in the smartphone to a transaction authentication server without revealing the exact price of any product item, wherein the transaction authentication server utilizes the transaction detail data to conduct risk management processing of the transaction" --Specification on page 10, line 32 to page 11, line 3; and in FIG. 5.

"Receiving, by the smartphone processor, a response message from the transaction authentication server indicating the transaction has been authenticated in response to the transmitted transaction detail data; and" --Specification on page 10, line 32 to page 11, line 1; on page 19, lines 5-6 (the Abstract); and in FIG. 5.

"Transmitting, by the smartphone processor running the merchant wallet application in response to the response message, payment credential information stored in a storage device of the smartphone to at least one of (a) the merchant POS terminal operated by the merchant; and (b) a payment processor acting for the merchant." --Specification on page 12, lines 11-19; on page 19, lines 6-8; and in FIG. 5.

Claim 10 (independent)

"A method for enhancing the capability to detect and prevent fraudulent purchase transactions comprising:" – Specification on page 11, lines 30-34; and in FIG. 5.

"Receiving, in a computer from a smartphone comprising a smartphone processor running a merchant wallet application issued by a merchant, an indication that the smartphone processor performed a user authentication procedure in connection with a transaction between the smartphone and the merchant, wherein the indication specifies a type of use authentication procedure" – Specification on page 5, lines 28-31; on page 10, lines 19-20; on page 11, lines 17-20; and in FIG. 5.

"Receiving, in the computer from the smartphone processor, transaction detail data generated by the smartphone processor running the merchant wallet application, wherein the transaction detail data comprises identification data of each product item being purchased and respective price range data for each identified product item without revealing the exact price of any product item" --Specification on page 10, lines 32 to page 11, line 1; on page 11, lines 5-15; and in FIG. 5.

"Performing, by the computer, risk management processing of the transaction utilizing the transaction detail data and based at least in part on the indication that the smartphone processor performed a user authentication procedure in connection with the transaction" --Specification on page 10, lines 21-25; on page 11, lines 15-30; and in FIG. 5.

"Authenticating, by the computer based on the risk management processing, the transaction; and" --Specification on page 12, lines 4-5.

"Transmitting, by the computer to the smartphone processor running the merchant wallet application, a response message indicating the transaction has been authenticated." --Specification on page 10, line 32 to page 11, line 1; on page 19, lines 5-6 (Abstract); and in FIG. 5.

Claim 16 (independent)

"A method for enhancing the capability to detect and prevent fraudulent purchase transactions comprising:" – Specification on page 11, lines 30-34; and in FIG. 5.

"Transmitting, by a smartphone processor of a smartphone to a remote computer, an indication that the smartphone performed a user authentication procedure in connection with a transaction between the smartphone and a merchant, wherein the indication specifies a type of user authentication procedure" – Specification on page 5, lines 28-31; on page 10, lines 19-20; on page 11, lines 17-20; and in FIG. 5.

"Generating, by the smartphone processor running a merchant wallet application, transaction detail data comprising identification data of each product item being purchased from the merchant in the transaction and respective price range data for each identified product item without revealing the exact price of any product item" --Specification on page 10, lines 32 to page 11, line 1; on page 11, lines 5-9; and in FIG. 5.

"Transmitting, by the smartphone processor via the internet, the transaction detail data to the remote computer for use in conducting risk management processing of the transaction, the remote computer operated by one of: (a) a payment account issuer and (b) a transaction authentication service" --Specification on page 3, lines 27-31; on page 10, line 32 to page 11, line 3; and in FIG. 5.

"Receiving, by the smartphone processor, an indication that the remote computer has authenticated the transaction; and" --Specification on page 10, line 32 to page 11, line 1; and in FIG. 5.

"Transmitting, by the smartphone processor running the merchant wallet application in response to the indication, payment credential information stored in a storage device of the smartphone to at least one of the merchant POS terminal operated by the merchant and a payment processor acting for the merchant." --Specification on page 12, lines 11-19; on page 19, lines 6-8; and in FIG. 5.

GROUNDS OF REJECTIONS TO BE REVIEWED ON APPEAL

(1) 35 U.S.C. §101 Rejection

Claims 1, 4-10, 13, 14, 16 and 18 stand rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter.

ARGUMENT

I. Applicable Law

The current jurisprudence regarding 35 U.S.C. §101 stems from the prominent Supreme Court decision in *Alice Corporation Pty. Ltd. v. CLS Bank International, et al.*[7] (hereinafter "*Alice*"). In summary, the rule expressed in the *Alice* decision was that for certain types of claims, if the claim is directed to an "abstract idea" then it is patent-eligible only if it contains additional claim elements that amount to "significantly more" than the abstract idea itself.

Alice made no major changes to the framework for determining patent eligibility. In particular, the Court in *Alice* recognized the three judicially created exceptions to the coverage of Section 101: laws of nature, natural phenomena, and abstract ideas.[8] The Court also stated that the concern driving the exclusionary principal is "one of pre-emption" or, in other words, a concern "that patent law not inhibit further discovery by improperly tying up the future use of these building blocks of human ingenuity."[9]

The Court in *Alice* did not provide any guidance regarding what constitutes an "abstract idea" within the meaning of the judicial exception. Instead, the Court cautioned against applying the judicial exceptions to patent eligible subject matter too loosely, in order to avoid the exceptions "swallow[ing] all patent law."[10] Moreover, in refusing to set a limit on what an abstract idea might be, the Court warned that "at some level, all inventions embody, use, reflect, rest upon, or apply . . . abstract ideas."[11] It was also noted that a claimed invention is not rendered non-statutory subject matter just because there is an abstract concept within the claims, and the Court clearly stated that "[a]pplication of such concepts 'to a new and useful end,' . . . remain eligible for patent protection."[12]

In view of the *Alice* decision and other decisions concerning Section 101, the U.S. Patent and Trademark Office (the "USPTO" hereinafter) promulgated several "Guidance" and "Update"

---

[7] 134 S.Ct. 2347 (2014).
[8] *Id.* at 134 S. Ct. 2347, 2354.
[9] *Id.* at 2354.
[10] *Id.* at 2357.
[11] *Id.* at 2357 (quoting *Mayo Collaborative Services v. Prometheus Labs.*, 566 U.S. 66, 132 S.Ct. 1289, 1293 (2012)).
[12] *Id.* at 2354 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)).

documents and then developed a two-step "*Alice/Mayo*" test[13] or framework. Step 1 of the framework involves determining whether the claim is directed towards one of the four statutory classes (i.e., process, machine, manufacture, or composition of matter). If so, then Step 2A requires determining whether the claim is directed to a judicial exception (i.e., laws of nature, natural phenomena, and abstract ideas). After a determination is made that the claims are directed to an abstract idea, then Step 2B requires determining whether the claim as a whole is patent-eligible due to additional elements that are sufficient to amount to "significantly more" than the abstract idea itself.[14]

In a Federal Register notice dated January 7, 2019, the USPTO issued revised guidelines in the form of a "Revised Patent Subject Matter Eligibility Guidance" document (the "2019 PEG" hereinafter).[15] The 2019 PEG focused on the application of the *Alice/Mayo* test and in particular addressed application of Step 2A of the *Alice/Mayo* analytical framework for determining whether claims are patent eligible. Specifically, the 2019 PEG revised the procedures for determining whether a patent application claim is directed to a judicial exception under step 2A of the *Alice/Mayo* test in two ways.

First, the 2019 PEG explains that abstract ideas under Step 2A, Prong 1 can be grouped as mathematical concepts, certain methods of organizing human activity, and mental processes. The 2019 JPEG notes that claims that do not recite subject matter that falls within these enumerated groupings of abstract ideas should not be treated as reciting abstract ideas,[16] except in a rare circumstance which requires a special procedure for analyzing the claim that should be followed.[17] The special procedure includes bringing the patent application to the attention of the Technology Center Director and providing justification for why such claim limitation is being treated as reciting an abstract idea. Thus, if the claim does not recite a judicial exception at Step 2A, Prong 1 then the claim recites patent-eligible subject matter.

Second, the 2019 PEG directs that under Step 2A, Prong 2 a patent application claim that recites a judicial exception is not "directed to" the judicial exception if the judicial exception is

---

[13] Derived from the *Alice* case and from *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66 (2012).
[14] See *2014 Interim Eligibility Guidance Quick Reference Sheet.*
[15] 84 Fed. Reg. No. 4, pages 50-57 (January 7, 2019).
[16] Emphasis added; *Id.* at pages 56-57.
[17] *Id.* in Section III.C of the 2019 PEG.

integrated into a practical application of the judicial exception.[18] Per the Manual of Patent Examination Procedure (MPEP),[19] the "directed to" inquiry requires that the character of a claim as a whole must be directed to a patent ineligible concept. In determining that the disclosed invention improves technology, "it is critical that examiners look at the claim "as a whole", in other words, the claim should be evaluated 'as an ordered combination, without ignoring the requirements of the individual steps.'" Also, "When performing this evaluation, examiners should be 'careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims."[20]

Thus, a claim is deemed patent-eligible under Prong 2 of Step 2A when that claim integrates a judicial exception (such as an abstract idea) into a practical application of the judicial exception. Integration into a practical application occurs when a claim imposes a meaningful limit on the judicial exception such that the judicial exception would not be monopolized by the claim.

A claim that recites a judicial exception, and where the judicial exception is not integrated into a practical application, is "directed to" the judicial exception under Step 2A and must then be evaluated under Step 2B of the *Alice/Mayo* test (inventive concept) to determine the subject matter eligibility of the claim.[21] The 2019 PEG therefore left unchanged the guidance provided by the USPTO regarding "Step 2B" as set forth in a USPTO Memorandum dated April 19, 2018 (the "Berkheimer Memorandum"), which was prompted by the Federal Circuit decision in *Berkheimer v. HP, Inc.*[22]

According to the *Berkheimer* decision, the question of whether certain claim limitations represent well-understood, routine, conventional activity raises a factual issue. Thus, the Berkheimer Memorandum requires Examiners to adduce factual evidence to support any finding that additional claim elements beyond an "abstract idea" do not amount to "significantly more" than the abstract idea. Section III.A. of the Berkheimer Memorandum sets forth an exclusive list

[18] Emphasis added; 84 Fed. Reg. No. 4, at page 50.
[19] See MPEP, Section 2106.04.
[20] *See, e.g.*, M.P.E.P. 2106.05(a) (citing *McRo*, 837 F.3d at 1313, 120 USPQ2d at 1100).
[21] *Id.* at page 50.
[22] *Berkheimer v. HP, Inc.*, 881 F.3d 1360 (Fed. Cir. 2018).

of the types of evidence that may be cited in support of an Examiner's finding that a claim element is well-understood, routine and conventional.

Appellant also draws the Board's attention to the following cases:

- *Uniloc v. LG Electronics*[23] The Court of Appeals for the Federal Circuit (CAFC) noted that the §101 inquiry "often turns on whether the claims focus on specific asserted improvements in computer capabilities or…an abstract idea for which computers are invoked merely as a tool." The CAFC then reiterated that software claims can be eligible when "they are directed to improvements to the functionality of a computer or network platform itself."[24] In the *Uniloc* case, the CAFC concluded that the claims overcame the Section 101 rejection as the claimed invention involves "the reduction of latency experienced by parked secondary stations in communication systems." Notably, the additional data field facilitates this improvement and changes the normal operation of the communication itself "to overcome a problem specifically arising in the realm of computer networks."[25] Ultimately holding that the claims are directed towards patent-eligible subject matter, the CAFC also stated: "Claims need not articulate the advantages of the claimed combinations to be eligible,"[26] and that "the claimed invention's compatibility with conventional communication systems does not render it abstract. Nor does the fact that the improvement is not defined by reference to "physical" components…Our precedent is clear that software can make patent-eligible improvements to computer technology, and related claims are eligible as long as they are directed to non-abstract improvements to the functionality of a computer or network platform itself."[27]

- *Cosmokey Solutions GMBH & CO. v. Duo Security LLC.*[28] The CAFC reversed a lower Court's finding that claims were ineligible for patent protection under 35 U.S.C. §101 holding that the claims were eligible at step two for reciting a specific improvement to authentication:

[23] Case 19-1835 (Fed. Cir. 2020). 957 F.3d 1303 (2020)
[24] *Id.* at pages 4-5.
[25] *Id.* at page 7.
[26] *Id.* at pages 9-10.
[27] Emphasis added; *Id.* at page 10.
[28] 15 F.4th 1091 (Fed. Cir. 2021); CAFC Case: 20-2043, October 4, 2021

> "The specification explains that these features in combination with the other elements of the claim constitute an improvement that increases computer network security, prevents a third party from fraudulently identifying itself as the user, and is easy to implement and can be carried out even with mobile devices of low complexity…Here, as the specification itself makes clear, the claims recite an inventive concept by requiring a specific set of ordered steps that go beyond the abstract idea identified by the district court and improve upon the prior art by providing a simple method that yields higher security."[29]

The Patent Office recognizes that: "even if one or more additional elements are well-understood, routine, conventional activity when considered individually, the combination of additional elements may amount to an inventive concept."[30] In addition, "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces."[31]

As will be discussed in more detail below, Appellant argues (a) that the Examiner erred in applying Step 2A, Prong 1 to the claims, and therefore that the claims are not directed to an "abstract idea"; and/or (b) that the Examiner erred in applying Step 2A, Prong 2, and thus the claims are patent-eligible under Section 101; and/or (c) that the Examiner failed to adduce the evidence required under Step 2B in accordance with the Berkheimer Memorandum and thus failed to show that certain claim elements are well-understood, routine and conventional.

[29] *Id.* at page 14.
[30] See MPEP, 2106.05(d).
[31] *Id.* at MPEP, 2106.05 I., citing to *BASCOM Global Internet v. AT&T Mobility LLC*, 827 F.3d 1341, 1350, 119 USPQ2d 1236, 1242 (Fed. Cir. 2016)

II. The Claims Are Subject-Matter-Eligible Under 35 U.S.C. §101

The Office tacitly admits that the claims fall within a statutory category of invention, namely a method or process, as there is no indication otherwise.[32]

Specifically, claims 1 and 4-9 recite a method of operating a smartphone running a merchant wallet application to enhance the capability for detecting and preventing fraudulent purchase transactions; claims 10, 13 and 14 are directed to a process for enhancing the capability of a computer to detect and prevent fraudulent purchase transactions; and claims 16 and 18 recite a method for enhancing the capability of a smartphone computer to detect and prevent fraudulent purchase transactions. Thus, all of the claims fall within a statutory category of invention.

Pending claims 1, 4-10, 13, 14, 16 and 18 stand or fall together concerning subject matter eligibility. Claim 1 is representative and thus may be taken as exemplary of all of the claims.

As mentioned above, claim 1 is directed to a method of operating a smartphone running a merchant wallet application to enhance the capability for detecting and preventing fraudulent purchase transactions. The method features a smartphone processor running a merchant wallet application receiving, via a near-field communication (NFC) component from a merchant point of sale (POS) terminal, an electronic receipt including data identifying purchased items and a price per item.

The smartphone processor then generates, based on the data of the electronic receipt, transaction detail data comprising identification data of each product item being purchased and respective price range data for each identified product item.

Next, the smartphone processor transmits, from the merchant wallet application in the smartphone via the internet to a transaction authentication server, the transaction detail data without revealing the exact price of any product item, wherein the transaction authentication server utilizes the transaction detail data to conduct risk management processing of the transaction.

The smartphone processor then receives a response message from the transaction authentication server indicating the transaction has been authenticated in response to the transmitted transaction detail data, and in response to the response message, transmits payment

[32] See Final Action, pages 4-6, items 6-7.

credential information stored in a storage device of the smartphone to at least one of (a) the merchant POS terminal operated by the merchant and (b) a payment processor acting for the merchant.[33]

In the following remarks, Appellant respectfully contends that the Examiner's arguments are erroneous and consequently that the Section 101 rejection of claims 1, 4-10, 13, 14, 16 and 18 should be reversed.

A. The claims are not directed to a judicial exception

The 2019 PEG[34] promulgated by the U.S. Patent Office explains that abstract ideas can be grouped as mathematical concepts, certain methods of organizing human activity, and mental processes, and states that claims that do not recite subject matter falling within one of these enumerated groupings should not be treated as reciting an abstract idea.[35]

The Examiner, under Step 2A, Prong 1 of the *Alice/Mayo* test, paraphrased the elements of claim 1 (leaving out important details) and then asserted, without any support or explanation, that the paraphrased limitations are directed to "concepts of organizing human activity via use of generic computer components."[36] The Office then stated: "Hence, it falls within the 'Certain Methods of Organizing Human Activity' grouping of abstract ideas. Accordingly, the claim recites an abstract idea."[37]

Appellant respectfully submits that the allegation made by the Office that claim 1 is directed to an abstract idea is insufficient as it identifies a concept as a judicial exception by over-generalizing the claim and simplifying it into its "gist" or core principles. In particular, the "directed to" inquiry of Step 2A, Prong 1 of the *Alice/Mayo* test requires that the character of a claim as a whole is directed to a patent ineligible concept.[38] In determining that the disclosed invention improves technology, "it is critical that examiners look at the claim 'as a whole', in other words, the claim should be evaluated 'as an ordered combination, without ignoring the

[33] See pending claim 1.
[34] Federal Register, Vol. 84, No. 54, pages 51-57 (January 7, 2019).
[35] Emphasis added; *Id.* at page 50.
[36] Final Action at page 4, lines 17-25.
[37] Id. at page 4, lines 25-27.
[38] See Manual of Patent Examination Procedure (MPEP) Section 2106.04

requirements of the individual steps.'" In addition: "When performing this evaluation, examiners should be 'careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims."[39]

It is submitted that the Examiner erred because claim 1 was not evaluated as an ordered combination while also not ignoring requirements of the individual steps. In particular, the process recited by claim 1 solves the technological problem of how to electronically provide transaction detail data, including a useful indication of item pricing, to an authentication server without revealing the exact price of any product item, so that the authentication server can apply reliable and sophisticated risk management algorithms to the transaction involving a smartphone and a merchant POS terminal.[40] These goals are achieved by having the smartphone processor running the merchant wallet application generate transaction detail data, based on the data of an electronic receipt received from the POS terminal, which data incudes identification data of each product item being purchased and respective price range data. Next, the smartphone processor transmits that transaction detail data via the internet to a transaction authentication server without revealing the exact price of any product item. The transaction authentication server then utilizes the transaction detail data to conduct risk management processing.[41]

The claimed process therefore advantageously provides added assurance to an issuer that the transaction is legitimate in a manner that is transparent to the user, and the payment transaction may then proceed according to terms that are favorable to the merchant (concerning factors such as interchange and/or shifting of liability to the issuer) in case the transaction ultimately proves to be problematic.[42]

Appellant maintains that the Office ignored the requirements of claim 1 concerning the smartphone processor running the merchant wallet application generating transaction detail data comprising identification data of each product item being purchased and respective price range data for each identified product item, and then transmitting the transaction detail data via the internet to a transaction authentication server without revealing the exact price of any product item, wherein the transaction authentication server utilizes the transaction detail data to conduct

[39] *Id.* at M.P.E.P. 2106.05(a) (citing *McRo*, 837 F.3d at 1313, 120 USPQ2d at 1100).
[40] See published U.S. application (US 2018/0032996) at paragraphs 0060 and 0062.
[41] *Id.* at paragraph 0062.
[42] *Id.* at paragraph 0018.

risk management processing of the transaction. It is therefore respectfully submitted that the Office failed to establish a *prima facie* case under Prong 1 of Step 2A of the *Alice/Mayo* test.

Furthermore, Appellant submits that the features of claim 1 cannot be considered as falling within the enumerated Certain Methods of Organizing Human Activity grouping of abstract ideas, at least because the claimed subject matter is not a fundamental economic principle or practice. Claim 1 instead is directed to a method of operating a smartphone running a merchant wallet application which engages in a transaction with a merchant's POS terminal, wherein a smartphone processor receives an electronic receipt, generates transaction detail data comprising product item identification and a respective price range for each product item, and then transmits the transaction detail data to a transaction authentication server without revealing the exact price of any product item. The smartphone processor also receives a response message from the authentication server indicating transaction authentication, and then transmits payment credential information stored in a storage device of the smartphone to at least one of the merchant POS and a payment processor.

Appellant respectfully maintains that such processing is not a fundamental economic practice (it is a technological activity), nor is it a commercial or legal interaction, nor is it a technique for managing personal behavior or relationships or interactions between people. Instead, the elements of claim 1 are directed to a process involving electronic components (a smartphone processor running a merchant wallet application, a merchant POS terminal, a transaction authentication server, a storage device of the smartphone, and a payment processor) which enables a smartphone to provide transaction detail data, including a useful indication of item pricing, to an authentication server without revealing the exact price of any product item, so that the authentication server can apply reliable and sophisticated risk management algorithms to the transaction in a manner that is transparent to the user.[43] Thus, claim 1 is directed to statutory subject matter.

Yet further, the Office has not articulated any reason(s) why the limitations of claim 1 should be considered as falling within the "Certain Methods of Organizing Human Activity" category. Instead, a bald assertion was made that the limitations of claim 1 "are directed to concepts of organizing human activity" apparently because the content of the operation relates to

[43] See U.S. published application (US2018/0032996) at paragraphs 0060 and 0062.

a transaction between a smartphone and a merchant POS terminal. However, the claims (and the disclosure of this application) are not directed to the fundamental idea of conducting a purchase transaction as explained above. Claim 1 is instead directed to a process for operating a smartphone running a merchant wallet application for enhancing the capability for detecting and preventing fraudulent purchase transactions. Therefore, the features of claim 1 are not directed to a judicial exception under Step 2, Prong 1.

Moreover, the limitations of claim 1 are directed to a process that enables a smartphone to provide transaction detail data, including a useful indication of item pricing, to an authentication server without revealing the exact price of any product item. As a result, the authentication server can beneficially apply reliable and sophisticated risk management algorithms to the transaction in a manner that is transparent to the user. As recognized by the Court in *Uniloc,* "Claims need not articulate the advantages of the claimed combinations to be eligible," and 2. "the claimed invention's compatibility with conventional communication systems does not render it abstract. Nor does the fact that the improvement is not defined by reference to "physical" components…Our precedent is clear that software can make patent-eligible improvements to computer technology, and related claims are eligible as long as they are directed to non-abstract improvements to the functionality of a computer or network platform itself." Appellant therefore respectfully submits that claim 1 is directed to non-abstract improvements to the functionality of a smartphone which operates to provide transaction detail data, including a useful indication of item pricing, to an authentication server without revealing the exact price of any product item, and thus it recites patent-eligible subject matter.

In view of the above remarks, Appellant respectfully submits that claim 1 is not directed to the "Certain Methods of Organizing Human Activity" grouping of abstract ideas and thus not directed to a judicial exception, and that the Examiner's interpretation of Prong 1 of Step 2A represents a clear deficiency in the *prima facie* case of the present rejection under 35 U.S.C. §101. Consequently, Appellant respectfully requests this Honorable Board to reverse the 35 U.S.C. §101 rejection of the claims.

B. The pending claims integrate the exception into a practical application and therefore pass Step 2A, Prong 2 of the Alice/Mayo *test*

Even if, solely for the sake of argument (and not conceded), claim 1 could be viewed as reciting an abstract idea at Step 2A, Prong 1, Appellant submits that claim 1 is directed to a practical application of the abstract idea under Prong 2 and thus recites patent-eligible subject matter.

The 2019 PEG explains that, under Step 2A, Prong 2 of the *Alice/Mayo* test, a claim that recites a judicial exception is not "directed to" the judicial exception if the judicial exception is integrated into a practical application of the judicial exception.[44] This occurs if the claim imposes a meaningful limit on the judicial exception such that the claim does not monopolize the judicial exception.

As explained in Appellant's specification, at the time the invention was made the inventors recognized that opportunities existed to enhance the capability to detect and prevent fraud in situations where a smartphone running a wallet application is utilized to conduct a payment transaction with a merchant POS terminal.[45] Accordingly, the claimed process enables a smartphone processor running a merchant wallet application to engage in a transaction with the merchant's POS terminal, receive an electronic receipt, generate transaction detail data comprising product item identification and a respective price range for each product item, and then transmit the transaction detail data to a transaction authentication server without revealing the exact price of any product item. The process permits the transaction authentication server to use the transaction detail data to conduct risk management processing, as recited by claim 1. The method continues with the smartphone processor receiving a response message from the transaction authentication server indicating transaction authentication, and then transmitting payment credential information stored in a storage device of the smartphone to at least one of the merchant POS and a payment processor.

The Examiner alleged that the judicial exception is not integrated into a practical application because the additional elements are "generic computer components" recited "at a

---

[44] Emphasis added; 84 Fed. Reg. No. 4, at page 50.
[45] See U.S. published application (US2018/0032996) at paragraphs 0011 and 0062.

high level of generality" and thus the additional elements do not impose any meaningful limits on practicing the abstract idea.[46] Appellant respectfully disagrees.

Appellant notes that the Examiner failed to demonstrate that the specific steps recited in claim 1 pre-empt all inventions concerning "a transaction detail data sharing process" (the alleged abstract idea) and instead merely quoted boilerplate language provided by the U.S. Patent Office in the 2019 PEG to describe and then dismiss the claim elements. Specifically, the Examiner alleged that claim 1:

> "… only recites additional elements of a smartphone, a processor, a point of sale terminal, a server and a payment processor to perform operations. The generic computer components are recited at a high-level of generality (performing generic computer functions) such that it amounts no more than mere instructions to apply the exception using generic computer components."[47]

Appellant notes, however, that the as-filed Detailed Specification indeed explains, with reference to the process depicted in FIG. 5, how the elements of claim 1 improve the operation of the smartphone processor:

> "…At **506**, the wallet app **311** transmits transaction data, such as transaction detail data, to the authentication server **206**. … In some embodiments, the transaction detail data may also include, for each purchased product item, an indicator of a particular price range that represents the purchase price for the product item in question. ***In this way, it is possible to give the issuer/authentication service a useful indication of the item price without revealing the exact price of the item***…"[48]

> "Transmission of the transaction detail data may occur via communication between the mobile device **202** and the authentication server **206**. …In addition to sending transaction data, including transaction detail data, to the authentication server **206**, ***the mobile device 202 may also send other data to the authentication server that may aid the authentication server in its risk management processing***."[49]

> "At **508**, the authentication server **206** may perform risk management processing relative to the current transaction. The authentication server **206** may use some or all of the information provided by the wallet app **311** in connection with step **506**, as just described. ***With this information, including product and price range detail, the authentication server 206 may be able to run more reliable and***

[46] Final Action, page 5, lines 1-11.
[47] Final Action, page 5, lines 2-5.
[48] Emphasis added; See U.S. published application (US2018/0032996) at paragraph 0060.
[49] Emphasis added: *Id.* at paragraph 0061.

> ***sophisticated risk management algorithms than are typically performed by an account issuer with respect to a transaction. Thus the authentication server 206 may have an enhanced capability for detecting and preventing fraudulent transactions, due at least in part to the transaction detail data shared from the merchant wallet app 311***. With this added assurance to the issuer that the transaction is legitimate, the payment transaction may proceed according to terms that are favorable to the merchant relating to factors such as interchange and/or shifting of liability to the issuer in case the transaction ultimately proves to be problematic."[50]

Accordingly, Appellant respectfully suggests that, just like in the *Uniloc* case (cited herein above), the present claims are patent eligible at Step 2A, Prong 2 because claim 1 recites a specific improvement to the functionality of a smartphone processor of a smartphone which enables an enhanced capability for detecting and preventing a fraudulent purchase transaction because the present specification explains that the combinations of elements in claim 1 constitute an improvement over conventional methods. Thus, as made clear in the specification, claim 1 recites an inventive concept by requiring a specific set of ordered steps that go beyond the abstract idea and improves upon the prior art.

Furthermore, Appellant respectfully maintains that fundamentally, the instant claims are not designed to monopolize "transaction detail data sharing processes" which the Office specified as constituting the abstract idea.[51] In other words, the claims will not "tie up" the excepted subject matter and pre-empt others from using the law of nature, natural phenomenon or abstract idea. Moreover, the Office failed to demonstrate how the specific steps recited in the claims would pre-empt all inventions concerning "transaction detail data sharing processes."

Yet further, Appellant submits that claim 1 imposes at least one meaningful limit on the abstract idea of "transaction detail data sharing processes," and thus would not monopolize it. For example, claim 1 requires: "*generating, by the merchant wallet application running in the smartphone based on the data of the electronic receipt* (received from the merchant POS), *transaction detail data comprising identification data of each product item being purchased and respective price range data for each identified product item"* before transmitting the transaction detail data to a transaction authentication server *without revealing the price of any product item*.

---

[50] Emphasis added; *Id.* at paragraph 0062.
[51] Final Action, at page 4, line 17.

Thus, claim 1 would not cover, for example, a process of "transaction data sharing processes" that did not generate such transaction detail data and/or that would transmit transaction detail data that includes the price of one or more product items. Consequently, claim 1 imposes a meaningful limit on the alleged judicial exception and thus integrates it into a practical application.

Accordingly, in view of the above remarks, Appellant submits that the Examiner erred in the application of Step 2A, Prong 2 of the *Alice/Mayo* test, and thus requests this Honorable Board to reverse the Section 101 rejection of claims 1, 4-10, 13, 14, 16 and 18 for at least this additional reason.

C. The elements of claims are not "well-understood, routine and conventional"

The Examiner treats Step 2B of the subject matter eligibility analysis framework in a cursory and conclusory manner. Specifically, the entire rejection under Step 2B reads as follows:

> "Next the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than an abstract idea. Claim 1 does not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional elements to perform operations amount to no more than mere instructions to apply the exception using generic computer components. Mere instruction to apply an exception using generic computer components cannot provide an inventive concept. The claim is not patent eligible."[52]

Appellant observes that there is no evidence in the record of the technology recited by the claims being well-known at the time of filing or simply involving performance of "well-understood, routine, and conventional activities commonly used in the industry." The Examiner has simply made reference to an earlier recitation of the claim language and failed to satisfy the mandate of *Berkheimer* and determine, as a matter of fact that claim 1, when considered as an ordered combination is "well-understood, routine and conventional." Consequently, the Examiner fell short in applying Step 2B of the *Alice/Mayo* test and so failed to lay a proper foundation for finding that claim 1 is not patent-eligible.

[52] Final Action at page 5, lines 12-18.

Moreover, the claims do not recite computer functions that are "well-understood, routine, conventional activit[ies]" previously known to the industry."[53] The claims do not merely describe "a transaction detail data sharing process" as asserted by the Examiner. To the contrary, the claims go well beyond this idea by *extensively incorporating* additional features as described above. Further, an inventive concept **is** provided by the claims as there are **no outstanding prior art rejections** cited against the claimed features. In fact, the Examiner acknowledged that the pending claims are non-obvious under Section 103 over the prior art of record.[54]

Appellant further notes that whether or not specific claim features are sufficient to amount to significantly more than the judicial exception itself, is a factual analysis that must be based on evidence. The standard of review applied to findings of fact is the "substantial evidence" standard under the Administrative Procedure Act ("APA"), 5 U.S.C. 500 et seq. As noted above, there are **no outstanding art rejections** cited against the claimed features, making the claimed invention novel and non-obvious. Because no art discloses or suggests at least the features of claim 1, the features of claim 1 are not "well-understood, routine and conventional," and as such, it clearly recites "significantly more" than the allegedly well-known abstract idea put forth by the Examiner.

In view of the above remarks, Appellant submits that the Office fell short in applying Step 2B of the *Alice/Mayo* test. Consequently, Appellant requests this Honorable Board to reverse the Section 101 rejection of the claims for at least this additional reason.

* * * * *

In summary, Appellant respectfully submits that the Examiner erred because claims 1, 4-10, 13, 14, 16 and 18 do not recite subject matter falling within one of the enumerated groupings of abstract ideas specified in the 2019 PEG, and thus are not directed to an abstract idea; and/or because the claims integrate the alleged abstract idea into a practical application that applies, relies on, and/or uses the abstract idea in a manner that imposes a meaningful limit on the abstract idea resulting in the claims reciting patent-eligible subject matter; and/or because the

[53] See, *Alice* at Section III.B.2.
[54] Final Action, page 8, item 12.

claims recite significantly more than the abstract idea and thus recite patent-eligible subject matter.

CONCLUSION

The 35 U.S.C. §101 rejections set forth in the Final Action are erroneous for the reasons set forth above. Consequently, Appellant respectfully requests this Honorable Board to reverse the Examiner's decision.

An Appendix A of claims involved in this appeal is attached hereto. No evidence is being submitted herewith, and thus Appendix B is empty. In addition, no prior or pending appeals, interferences, or judicial proceedings are known to Appellant, Appellant's legal representative, or assignee, which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal. Thus, there are no copies of decisions rendered by a Court or the Board to attach, and therefore Appendix C is empty.

If any issues remain, or if the Honorable Members of the Board or the Examiner have any further suggestions for expediting allowance of the present application, please contact the undersigned using the contact information provided below.

Respectfully submitted,

November 6, 2024
Date

/Stephan J. Filipek /
Stephan J. Filipek
Attorney for Appellant
Registration No. 33,384
Buckley, Maschoff & Talwalkar LLC
134 Main Street
New Canaan, CT 06840
Tel.: (203) 972-3460
Fax.: (203) 972-7627
filipek@bmtpatent.com

APPENDIX A – CLAIMS

1. A method of operating a smartphone running a merchant wallet application to enhance the capability for detecting and preventing fraudulent purchase transactions, the wallet application issued by a merchant, the method comprising:

receiving, by a processor of the smartphone running the merchant wallet application via a near-field communication (NFC) component from a merchant point of sale (POS) terminal, an electronic receipt including data identifying purchased items and a price per item;

generating, by the smartphone processor running the merchant wallet application based on the data of the electronic receipt, transaction detail data comprising identification data of each product item being purchased and respective price range data for each identified product item;

transmitting, by the smartphone processor, the transaction detail data via the internet from the merchant wallet application in the smartphone to a transaction authentication server without revealing the exact price of any product item, wherein the transaction authentication server utilizes the transaction detail data to conduct risk management processing of the transaction;

receiving, by the smartphone processor, a response message from the transaction authentication server indicating the transaction has been authenticated in response to the transmitted transaction detail data; and

transmitting, by the smartphone processor running the merchant wallet application in response to the response message, payment credential information stored in a storage device of the smartphone to at least one of (a) the merchant POS terminal operated by the merchant; and (b) a payment processor acting for the merchant.

2.-3. (canceled)

4. The method of claim 1, wherein the smartphone processor running the wallet application transmits to the transaction authentication server, prior to the receiving step, location data that indicates a current location of the smartphone.

5. The method of claim 1, wherein the smartphone processor running the wallet application transmits to the transaction authentication server, prior to the receiving step, device identification data that uniquely identifies the smartphone.

6. The method of claim 1, wherein the smartphone processor running the wallet application transmits to the transaction authentication server, prior to the receiving step, an indication that the smartphone has performed a user authentication procedure in connection with the transaction.

7. The method of claim 6, wherein the indication specifies a type of user authentication procedure.

8. The method of claim 1, further comprising:

prior to the transmitting step, receiving a digital receipt for the transaction, by the smartphone processor, from a merchant device at the point of sale.

9. The method of claim 8, wherein the smartphone processor extracts at least some of the transaction detail data from the digital receipt.

10. A method for enhancing the capability to detect and prevent fraudulent purchase transactions comprising:

receiving, in a computer from a smartphone comprising a smartphone processor running a merchant wallet application issued by a merchant, an indication that the smartphone processor performed a user authentication procedure in connection with a transaction between the smartphone and the merchant, wherein the indication specifies a type of use authentication procedure;

receiving, in the computer from the smartphone processor, transaction detail data generated by the smartphone processor running the merchant wallet application, wherein the

transaction detail data comprises identification data of each product item being purchased and respective price range data for each identified product item without revealing the exact price of any product item;

performing, by the computer, risk management processing of the transaction utilizing the transaction detail data and based at least in part on the indication that the smartphone processor performed a user authentication procedure in connection with the transaction;

authenticating, by the computer based on the risk management processing, the transaction; and

transmitting, by the computer to the smartphone processor running the merchant wallet application, a response message indicating the transaction has been authenticated.

11.-12. (canceled)

13. The method of claim 10, further comprising:

in response to a result of the risk management processing, generating a cryptogram by the computer; and

transmitting the cryptogram by the computer to (a) a merchant device associated with the transaction; or (b) a transaction processor associated with a merchant involved in the transaction.

14. The method of claim 10, wherein the risk management processing is based at least in part on device identification data received from the smartphone, the device identification data uniquely identifying the smartphone.

15. (canceled)

16. A method for enhancing the capability to detect and prevent fraudulent purchase transactions comprising:

transmitting, by a smartphone processor of a smartphone to a remote computer, an indication that the smartphone performed a user authentication procedure in connection with a transaction between the smartphone and a merchant, wherein the indication specifies a type of user authentication procedure;

generating, by the smartphone processor running a merchant wallet application, transaction detail data comprising identification data of each product item being purchased from the merchant in the transaction and respective price range data for each identified product item without revealing the exact price of any product item;

transmitting, by the smartphone processor via the internet, the transaction detail data to the remote computer for use in conducting risk management processing of the transaction, the remote computer operated by one of: (a) a payment account issuer and (b) a transaction authentication service;

receiving, by the smartphone processor, an indication that the remote computer has authenticated the transaction; and

transmitting, by the smartphone processor running the merchant wallet application in response to the indication, payment credential information stored in a storage device of the smartphone to at least one of the merchant POS terminal operated by the merchant and a payment processor acting for the merchant.

17. (canceled)

18. The method of claim 16, wherein the smartphone processor transmits, to the remote computer, prior to the receiving step, device identification data that uniquely identifies the smartphone.

19.-20. (canceled)

Appendix B – Evidence

No evidence is being submitted with this Appeal Brief (i.e., this appendix is empty).

Appendix C - Related Proceedings

No prior or pending appeals, interferences, or judicial proceedings are known to Appellant, Appellant's legal representative, or assignee, which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal. Therefore, there are no copies of decisions rendered by a Court or the Board to attach (i.e., this appendix is empty).