

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND
MASTERCARD INTERNATIONAL INCORPORATED,
Petitioner,

v.

OV LOOP, INC.,
Patent Owner.

IPR2023-01289
Patent 10,032,171 B2

Before JAMES A. TARTAL, RYAN H. FLAX, and BRENT M. DOUGAL,
Administrative Patent Judges.

TARTAL, *Administrative Patent Judge.*

DECISION
On Remand Following Director Review
Maintaining That All Challenged Claims Are Unpatentable
35 U.S.C. § 314

This Decision is issued pursuant to the Order Granting Director Review and Remanding to the Patent Trial and Appeal Board for Further Proceedings. Paper 41 (“Remand Order”). We previously determined that Mastercard Incorporated and Mastercard International Incorporated (“Petitioner”) establishes by a preponderance of the evidence that the subject matter of claims 1–33 (the “Challenged Claims”) of U.S. Patent No. 10,032,171 B2 (Ex. 1001, “the ’171 patent”) would have been obvious over Collinge¹. Paper 37 (“Final Written Decision” or “FWD”).

Following issuance of the Final Written Decision, OV Loop, Inc. (“Patent Owner”) requested Director Review only of our determination that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 10–13 and 27–30 of the ’171 patent would have been obvious over Collinge. Paper 39 (“DR Request” or “DR Req.”).² Petitioner opposed Patent Owner’s Request for Director Review. Paper 40 (“DR Req. Opp.”). In the Remand Order the Acting Director granted Patent Owner’s DR Request.

¹ U.S. Patent App. Pub. No. US 2013/0262317 A1, published Oct. 3, 2013 (Ex. 1011, “Collinge”). Petitioner establishes that Collinge was prior art as of the filing date of Provisional Application No. 61/619,095 (Ex. 1009, “the ’095 Provisional”). FWD 18–22. Collinge expressly incorporates by reference the ’095 Provisional. Ex. 1011 ¶ 1. For purposes of our analysis below, we refer at times to the ’095 Provisional with the understanding that the ’095 Provisional is included in Collinge by express incorporation.

² Not at issue here is our determination in the Final Written Decision that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 1–9, 14–26, and 31–33 of the ’171 patent would have been obvious over Collinge.

The Remand Order states that it was “unclear” in the Final Written Decision which components of Collinge “the Board relied on for claim 10’s limitation ‘receiving [at the remote computer system] an authorization request to authorize the transaction from the POS terminal.’” Remand Order 3. The Order instructs: “[o]n remand, the Board shall consider Patent Owner’s arguments as to claims 10 and 27, and their dependent claims. Regardless of the Board’s disposition on remand, the Board should address Patent Owner’s arguments and explain more fully its findings as to claims 10 and 27.” *Id.* The Remand Order further states that “this case is remanded to the Board for consideration of the arguments made in Patent Owner’s DR Request” and that we “should point more specifically to where in Collinge the argued limitation is taught, if anywhere, and which components of Collinge satisfy the limitation, if any.” *Id.*

As instructed, in this Decision we consider Patent Owner’s arguments raised in the DR Request as to claims 10 and 27, and their dependent claims.³ As explained in detail below, and consistent with our determination in the Final Written Decision, we conclude Petitioner establishes by

³ We consider the arguments presented in Patent Owner’s DR Request in the context of arguments presented in Patent Owner’s Response, as arguments on the merits may be considered waived unless presented in that Response. See Paper 16, 9 (explaining that “Patent Owner is cautioned that any arguments not raised in the response may be deemed waived”).

a preponderance of the evidence that the subject matter of claims 10–13 and 27–30 of the ’171 patent would have been obvious over Collinge.⁴

I. INTRODUCTION

A. *Summary of Procedural History*

Petitioner filed a Petition (Paper 1, “Pet.”) pursuant to 35 U.S.C. §§ 311–319 requesting an *inter partes* review of the Challenged Claims. We instituted an *inter partes* review of the Challenged Claims on all grounds of unpatentability asserted in the Petition. Paper 15. Patent Owner filed a Response. Paper 22 (“PO Resp.”). Petitioner filed a Reply to the Patent Owner Response. Paper 26 (“Pet. Reply”). Patent Owner filed a Sur-reply in support of the Patent Owner Response. Paper 29 (“PO Sur-reply”). In our Final Written Decision, we found Petitioner establishes that the subject matter of the Challenged Claims would have been obvious over Collinge. FWD 64.

A. *Illustrative Claims*

Dependent claims 10–13 and 27–30 are at issue on remand. Claim 10 depends from independent claim 1. Claims 11–13 further depend from claim 10. Claim 27 depends from independent claim 17. Claims 28–30 further depend from claim 27. Claims 1, 10, 17, and 27, reproduced below, are illustrative of the subject matter claimed and at issue here:

⁴ This Decision provides an explanation supplemental to the Final Written Decision pertaining to claims 10–13 and 27–30 of the ’171 patent, but does not alter any determination set forth in the Final Written Decision or our conclusion that Petitioner establishes by a preponderance of the evidence the unpatentability of each of claims 1–33 of the ’171 patent, as set forth in the Final Written Decision.

1. A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;

requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one

POS command communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and

storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

Ex. 1001, 50:61–51:65.

10. The method of claim 1, further comprising, at the remote computer system, performing an authorization process comprising:

- receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

- determining a current non-permanent cryptographic key associated with the account using the account identifier;

- calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

- verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

- sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

Id. at 52:42–61.

17. A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

- a mobile device comprising:

- a controller configured to route communications received over a communication channel from an electronic reader;

- a wireless interface to connect to a wireless network that is separate from the communications channel;

- a processor;

- a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application, when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, wherein the application does not have access to a permanent

cryptographic key issued for the digital credential and the application is executable to:

- request from the remote computer system, over the wireless network, a first set of data associated with the account;
- receive by the application, from the remote computer system over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;
- store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
- during an interrogation:
 - receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;
 - access the local cryptographic key associated with the account;
 - generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account use.cl to generate the response cryptogram;
 - and
 - respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation [sic], request from the remote computer system, over the wireless network, a second set of data associated with the account;
receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key associated with the account; and
store the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

Id. at 53:15–54:22.

27. The system of claim 17, further comprising, a remote computer system programmed to:
receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;
determine a current non-permanent cryptographic key associated with the account using the account identifier;
calculate a calculated cryptogram using the current nonpermanent cryptographic key associated with the account;
verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram;
and send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

Id. at 54:64–55:14.

B. Obviousness Based on Collinge

Petitioner contends the subject matter of claims 10–13 and 27–30 of the '171 patent would have been obvious over Collinge. Pet. 36–52, 58–61, 63–65; Pet. Reply 8–19. Petitioner relies on the

declaration testimony of Dr. Fiske in support of its contentions. *See, e.g.*, Ex. 1006 ¶¶ 81–113, 129–138, 144–161; Ex. 1050 ¶¶ 24–47.

According to the Remand Order, it was “unclear” from the Final Written Decision “which of Collinge’s components the Board relied on for claim 10’s limitation ‘receiving [at the remote computer system] an authorization request to authorize the transaction from the POS terminal.’” Remand Order 3. The Remand Order, highlighting Patent Owner’s pertinent arguments, states as follows:

Patent Owner argues [in the DR Request] that the Board erred because it relied on components of Collinge that were outside of Petitioner’s identified “remote computer system” to meet the functionality of the “remote computer system” of claim 10. *See* DR Request 1, 6–9, 11. In particular, Patent Owner argues that the Petition relies on Collinge’s disclosure that the point-of-sale (POS) terminal may transmit transaction information to acquirer processing server 312, yet Petitioner does not identify this server as part of the alleged “remote computer system” of claim 10. *See id.* at 7 (citing Pet. 58 (citing Ex. 1011 ¶ 77)).

Id. at 2. The Remand Order did not expressly address Petitioner’s opposition to the DR Request, which states that Patent Owner’s request was based on the “misleading assertion” that the Petition relied on processing server 312. DR Req. Opp. 1–2. As explained below, Petitioner shows that Collinge teaches a remote computer system that includes remote-SE system 110 (performing functions corresponding to the functions recited in the method of claim 1) and issuer processing server 308 (performing functions corresponding to the functions recited in the method of claim 10). Thus, Collinge’s component relied on “for claim 10’s limitation ‘receiving [at the remote computer system] an authorization request to authorize the transaction from the POS terminal’” is issuer processing server 308, which

Petitioner shows is a sub-part of the remote computer system of Collinge (a remote computer system that also includes remote-SE system 110 and is illustrated in Figure 7 of Collinge). Our analysis and discussion of Patent Owner's arguments in opposition are further detailed below.

1. *Dependent Claim 10*

As noted above, claim 10 depends from claim 1 and further recites “at the remote computer system, performing an authorization process.” “[T]he remote computer system” of dependent claim 10 is first recited by independent claim 1, which requires, in part, that a mobile device execute an “application” that requests and receives data “from a remote computer system” over a wireless network. Although Patent Owner does not dispute in its DR Request the sufficiency of Petitioner's showing in regard to claim 1, for proper context, we begin with a discussion of claim 1 before turning to the additional limitations of dependent claim 10.

With regard to claim 1's required exchange of data between the *mobile device* and the *remote computer system*, Petitioner shows that Collinge teaches a method whereby a mobile device requests and receives data *from a remote computer system*. Pet. 41–44. Specifically, Petitioner shows in regard to claim 1 as follows:

Collinge discloses that “[p]ayment credentials corresponding to the payment account may be stored in a remote-SE (remote-secure-element) system 110 for provisioning to the mobile device.” Pet. 38 (citing Ex[1011], [0042], [0071], Fig. 7; Ex[1009], [0061] (Table 1, Steps 1-2)). Further, “the mobile payment application 106 may transmit [a] CAP token to the remote-SE system 100,” Ex[1011], [0081], which causes the remote-SE system to generate and return payment credentials in an encrypted payload after verification of CAP token, *id.* at [0082]-[0083], [0085]. A [person of ordinary skill in the art] would understand that sending of CAP token initiates, and thus

constitutes a request for server to return payment credentials. Ex[1006] ¶ 87. Further, as shown in Collinge Fig. 7, the communication between the remote/cloud system to the phone is a different (second) communication channel (e.g., SSL/TLS) from the channel used to communicate with the POS reader/merchant (first communication channel, shown by the near-field communication symbols).

Pet. 38–39 (emphases omitted); *see also* FWD 30–31. Petitioner relies specifically on remote-SE system 110 as the sub-part of Collinge’s remote computer system that stores certain data exchanged with the mobile device, as required by claim 1 (i.e., “a digital credential” and “data associated with the account”), but, as can be seen in the portion of the Petition quoted above, the discussion of claim 1 in the Petition does not limit Collinge’s remote computer system to just remote-SE system 110. *See* Pet. 38–39. Moreover, Collinge expressly explains how remote-SE system 110 is only one sub-part of Collinge’s system for processing transactions remotely from the mobile device.

For example, Collinge identifies cloud-system 302 as a part of remote-SE system 110 through which the mobile payment application on the mobile device can connect with remote-SE system 110. *Id.* ¶¶ 42, 81; *see also id.* at ¶ 59 (referring to remote notification server 114 as “remote notification service 114”). Collinge explains that “cloud system 302 may store keys, payment credentials, and an application transaction counter, which may be provisioned from the cloud system 302,” and that “cloud system 302 may also transmit at least some of the information to the issuer 108.” *Id.* at ¶¶ 53–54; *see also* Pet. 26–28 (summarizing the operation of the system and method disclosed by Collinge).

Dependent claim 10 further requires, “at the remote computer system, performing an authorization process” comprised, in relevant part, of

receiving a request *from a POS terminal* and sending an authorization response *to the POS terminal*.” Thus, in claim 1 the recited method requires an exchange of data between the *mobile device* and the *remote computer system*, and, in dependent claim 10, the recited method further requires an exchange of data between the *POS terminal* and the *remote computer system*.

For claim 10, Petitioner shows that Collinge teaches a method whereby a POS terminal requests and receives the necessary data from a remote computer system. Pet. 41–44. In particular, Petitioner shows as follows:

Collinge discloses performing an authorization process at a payment network. Ex[1011], [0045], [0056]–[0057], [0086]–[0087]; *see also* Ex[1009], [0061] (Table 1, Steps 14–15).

...

Collinge discloses that the “point-of-sale terminal 120 may generate an authorization request for the payment transaction, which may include the UNREADER, the *generated CVC3 value* [*i.e.*, response cryptogram], the application transaction counter...” Ex[1011], [0086], [0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b), [0073], [0074]. Additionally, Collinge explains the POS terminal “may transmit the received payment information [from the mobile device] and any additional transaction information.” Ex[1011], [0077]. The authorization request would include an account identifier as that was a standard part of any authorization message, including the standard “m/chip” or mag stripe message mentioned in Collinge. Ex[1006] ¶ 129. Moreover, Collinge explains that the authorization response includes determining whether the transaction is authorized based on “available ... credit, etc. for the payment account”, and thus a [person of ordinary skill in the art] would understand the authorization request to contain the account identifier. Ex[1011], [0077].

To the extent not disclosed, a [person of ordinary skill in the art] would have found it obvious that the authorization request would include a response cryptogram and an account

because this is well established standard practice in the art and would be an obvious way to permit the issuer to authorize the transaction and associate it with the correct account. Ex[1037] at 57–58; Ex[1006] ¶ 131.

Collinge discloses that “the issuer processing server 308 may validate the payment CVC3 value using at least the UNREADER, UNCLOUD, and application transaction counter,” by retrieving (“determining”) the UNCLOUD and KSUN (hence the session key associated with the account and unique to transaction, as explained in [1.A-3]) values that were used by the Payment Credential Management System to generate (“calculating”) the CVC3 value. Ex[1011], [0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b). Because this CVC3 value is calculated using the same input and key—hence would be the same as—the CVC3 value included in the authorization request if the request originated from an authentic card, a [person of ordinary skill in the art] would understand that the “verifying” would simply involve comparing whether those two CVC3 values are the same. Ex[1037] at 58; Ex[1006] ¶ 132.

Also, as Collinge has acknowledged, “[m]ethods for validating a cryptogram will be apparent to persons having skill in the relevant art,” Ex[1011], [0077], and a [person of ordinary skill in the art] would have found it obvious to implement Collinge in the manner described above because these are standardized operations in secure payment transactions and are therefore applying a known technique (known message authentication code techniques) to yield predictable results (permit authentication). Ex[1006] ¶ 133.

Pet. 58–60 (emphases omitted).

In sum, Petitioner shows in the Petition that Collinge’s remote-SE system 110 is the component of the remote computer system that stores certain data exchanged with the mobile device, as required by claim 1, and Petitioner shows that Collinge’s interconnected issuer processing server 308 is the component of the remote computer system that receives a request from a POS terminal and sends an authorization response to the POS terminal, as required by claim 10. *Id.* at 38–44, 58–60.

2. *Patent Owner's Arguments in its DR Request*

Patent Owner presents two arguments in its DR Request. DR Req. 6–11. First, Patent Owner argues that the Final Written Decision “disregarded that the Petition relies on components from Collinge that are outside the [sic] of the alleged ‘remote computer system’ identified in Reply.” *Id.* at 6–9. Second, Patent Owner argues that there is “[n]o evidence that the components in Collinge identified for claim 10 are all part of a single remote computer system.” *Id.* at 9–11. We find these arguments unpersuasive for the reasons set forth in the Final Written Decision and further detailed below. *See* FWD 56–59.

a) *Whether the Petition Relies on components from Collinge Outside of the Alleged “remote computer system”*

In support of its argument that the Petition relies on components from Collinge outside of the alleged remoted computer system of Collinge, Patent Owner references an annotated version that Petitioner included in its Reply of Collinge’s Figure 7 from the ’095 Provisional, which we reproduce below.

server 308).⁵ See Ex. 1011 Fig. 7. Petitioner states in its Reply that “the Petition mapped functionality performed in at least the structures identified . . . in the blue box (which are expressly stated and shown to share a ‘connection 178’ therebetween) as corresponding to the functions of the remote computer system.” Pet. Reply 16–17 (citing Ex. 1009 ¶ 46, Fig. 7; Pet. 38–41, 58–59).

Patent Owner argues in its DR Request that “Petitioner did not show (or even allege) that the Blue-Box Structures perform every step of claim 10.” DR Req. 7. According to Patent Owner, “the Petition alleges only that elements outside of the blue box perform some of the recited steps

⁵ Collinge and the '095 Provisional each include “Figure 7” illustrating the same system. The Remand Order notes that Figure 7 in Collinge as published and Figure 7 in the '095 Provisional have “different item numbering and descriptions.” Remand Order 3 n.2. Any differences in these two figures are not material to our analysis. For example, in Collinge the element labeled “308” is identified as “issuer processing server” (a part of the “Issuer System”) and this component corresponds to the element labeled “180” in the '095 Provisional, which is identified as “issuer” (a part of the “Issuer System”). See Ex. 1009, ¶ 65, Fig. 7; Ex. 1011, ¶ 56, Fig. 7. Thus, when Petitioner refers to features of the “Issuer System” of Figure 7 of the '095 Provisional in its Reply (Paper 26), Petitioner is addressing the same elements of the “Issuer System” that appear in the same location of Figure 7 of Collinge as published, regardless of whether they have different item numbering. Similarly, Figure 7 of Collinge as published identifies remote-SE system 110 as a collection of components in a box with the heading “Cloud System.” The same collection of components are shown in Figure 7 of the '095 Provisional in a box with the heading “Cloud System,” but without an element number for a “remote-SE system.” Regardless of labeling, the relevant features of the systems disclosed in Figure 7 of Collinge as published and in Figure 7 of the '095 Provisional are identical for all purposes relevant to our analysis. See DR Req. 4 n.2 (Patent Owner acknowledging that “the Collinge Provisional [Ex. 1009] and Collinge [Ex. 1011] each include a substantially similar Figure 7”).

of claim 10,” and that “under the theory presented in the Petition, ‘acquirer processing server 312 of the acquirer 122’ are components of the alleged ‘*remote compute [sic] system,*’” both of which are located “outside of the Blue-Box Structures.” *Id.* From this, Patent Owner asserts that “the Petition does not show, nor even allege, that any such authorization request is received at the Blue-Box Structures from a “*POS terminal.*” *Id.* at 8. Patent Owner further asserts that “because the Board did not consider that Petitioner’s Blue-Box Structures explicitly exclude components in Collinge alleged to perform steps claimed “*at the remote computer system,*” the Board’s conclusion that Collinge renders obvious claim 10 is factually unsupported by the record.” *Id.* at 8–9.

Patent Owner’s arguments are not convincing because they are based on the mistaken premise that Petitioner alleges in the Petition that acquirer processing server 312 of Collinge, a component outside of the so-called “Blue-Box Structures,” performs steps of the method of claim 10. To the contrary, as explained above, Petitioner establishes that Collinge’s interconnected issuer processing server 308 is the component of the system that receives a request from a POS terminal and sends an authorization response to the POS terminal, as required by claim 10. *See* Pet. 38–44, 58–60. To further refute Patent Owner’s allegations, Petitioner explains that “neither the Petition, nor Reply (Paper 26), nor even Petitioner’s supporting expert declaration (Ex[1006]), ever mentions the “acquirer processing server 312.” DR Req. Opp. 2.

The Final Written Decision also addresses Patent Owner’s argument that Petitioner relied on parts of Collinge’s system beyond remote-SE System 110 in regard to the “remote computer system” of claim 10. In the Final Written Decision, we explain as follows:

Petitioner explains, and we agree, that Petitioner's identification of the remote computer system of Collinge was not limited to the "remote-SE system 110," but included other aspects of the Collinge computer system that Petitioner expressly relies upon, as shown in the annotated version of Collinge Figure 7 provided by Petitioner in Reply. Pet. Reply 16–18. We find no discrepancy in this regard with the portions of Dr. Fiske's testimony cited by Patent Owner, which does not suggest he relied on "different" remote computer systems to meet the additional limitations of claim 10. *See* PO Resp. 30 (citing Ex. 2035: 74:15-75:9); Pet. Reply. 18.

FWD 57.

Patent Owner's argument in the DR Request is premised primarily on Petitioner's citation to paragraph 77 of Collinge in the Petition. DR Req. 7. Patent Owner quotes language from paragraph 77 and asserts that "the Petition relies on Collinge's disclosure that "[t]he merchant point-of-sale terminal 120 may transmit the received payment information and any additional transaction information ... to the acquirer processing server 312 of the acquirer 122.'" DR Req. 7 (citing Pet. 58 (citing Ex. 1011 ¶ 77)). We are not convinced by Patent Owner's argument that by citing in the Petition to a paragraph from Collinge that addresses acquirer processing server 312, Petitioner implicitly "relied" on acquirer processing server 312, particularly because the Petition makes no mention of acquirer processing server 312. Moreover, paragraph 77 of Collinge also expressly addresses issuer processing server 308, the component of Collinge that Petitioner relies on as corresponding to the component that performs the recited functions of claim 10.

Specifically, paragraph 77 of Collinge refers to both issuer processing server 308 and acquirer processing server 312, stating, in part, as follows:

The merchant point-of-sale terminal 120 may transmit the received payment information and any additional transaction information (e.g., transaction amount, merchant identifier, etc.) to the acquirer processing server 312 of the acquirer 122. The acquirer processing server 312 may then generate and submit an authorization request for the financial transaction to the payment network 124. The payment network 124 may transmit relevant transaction data, such as the payment information and transaction amount, to the issuer processing server 308. The issuer processing server 308 may then validate the application cryptogram.

Ex. 1011 ¶ 77. In short, although paragraph 77 of Collinge is cited in the Petition and addresses both issuer processing server 308 and acquirer processing server 312, Petitioner relies on and shows that issuer processing server 308 (*not* acquirer processing server 312) receives “an authorization request to authorize the transaction from the POS terminal,” as required by claim 10. Pet. 58–59; Pet. Reply 16–18; DR Req. Opp. 2–4.

Furthermore, there is no dispute that in Collinge the “authorization process” is performed at issuer processing server 308 in response to a request it receives. Ex. 1011 ¶ 77 (“The issuer processing server 308 may then validate the application cryptogram”). Claim 10 requires “performing an authorization process” including “receiving an authorization request to authorize the transaction from the POS terminal” at the remote computer system. We recognize that acquirer processing server 312 facilitates receiving transaction information from the POS terminal and communicating an authorization request to the issuer processing server 308. *See* Ex. 1011 ¶ 77. It is merchant point-of-sale terminal 120, however, that transmits “the received payment information and any additional transaction information (e.g., transaction amount, merchant identifier, etc.) to the acquirer processing server 312,” so that “acquirer processing server 312 may then generate and

submit an authorization request for the financial transaction” through payment network 124 to issuer processing server 308 for validation. *Id.* Thus, Petitioner shows that in Collinge the request received by the issuer processing server 308 is “from” the POS terminal, as required by claim 10. *See* Pet. 58–6–; Ex. 1011, ¶ 77, Fig. 7.

We credit the testimony of Dr. Fiske in this regard, who explains as follows:

Collinge discloses that the “point-of-sale terminal 120 may generate an authorization request for the payment transaction, which may include the UNREADER, the generated CVC3 value, [i.e. response cryptogram], the application transaction counter...” Ex[1011], [0086]-[0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b), [0073]-[0074]. Additionally, Collinge explains the POS terminal “may transmit the received payment information [from the mobile device] and any additional transaction information.” Ex[1011], [0077]. The authorization request would include an account identifier as that was a standard part of any authorization message, including the standard “m/chip” or mag stripe message mentioned in Collinge. Moreover, Collinge explains that the authorization response includes determining whether the transaction is authorized based on “available ... credit, etc. for the payment account”, and thus a POSA would understand the authorization request to contain the account identifier. Ex[1011], [0077].

Ex. 1006 ¶ 130.

Accordingly, for purposes of showing how Collinge teaches or suggests the limitations of claim 10, Petitioner establishes that the issuer processing server 308 is part of the “remote computer system.” Pet. 58–60; Pet. Reply 16–18. Petitioner does not allege, and we need not resolve whether, acquirer processing server 312 is also part of the “remote computer system” of Collinge. In sum, Petitioner does not rely in the Petition on components from Collinge outside of the alleged “remote computer system,”

which Petitioner shows includes remote-SE system 110 in communication with issuer processing server 308.

b) *Whether Evidence Supports that the Components in Collinge Identified by Petitioner for Claim 10 are All Part of a Single “remote computer system”*

Because claim 10 expressly refers to “the remote computer system” of the “method of claim 1,” we understand from the Petition that Petitioner alleges remote-SE system 110 and processing server 308 are *both* sub-parts of Collinge’s system corresponding to the recited “remote computer system.” In other words, because Petitioner relies on both Collinge’s remote-SE system 110 and issuer processing server 308 (which are remote from the mobile device) as performing the recited steps of the “remote computer system,” Petitioner alleges in the Petition that both remote-SE system 110 and issuer processing server 308 are part of a single “remote computer system” of Collinge. Moreover, in response to arguments raised by Patent Owner in its Response, Petitioner explains in its Reply that remote-SE system 110 and issuer processing server 308 are both part of a “remote computer system” because they are connected and in communication. Pet. Reply 17–18 (citing Ex. 1009 ¶ 46, Fig. 7); *see also* Ex. 1011 ¶¶ 82, 84 (stating in regard to Figure 7 of Collinge that “the payment credentials management system 704,” a subpart of remote-SE system 110, “may be operated by or on behalf of the issuer 108, [which includes issuer processing server 308],” and that “the payment credentials management system 704 may perform a synchronization process with the issuer 108”).

Patent Owner argues that “Petitioner has presented no argument or evidence” that the components of Collinge relied on by Petitioner “together

constitute a single ‘*remote computer system.*’” DR Req. 9. According to Patent Owner, the Board’s “determination that claim 10 is obvious over Collinge” is “based on an implicit finding of material fact that all of the identified components in Collinge—which Collinge separately illustrates as a ‘Cloud System,’ ‘Issuer System,’ ‘Acquirer System,’ and “payment network” . . . are in fact a single “*remote computer system.*” *Id.* (citing FWD 59; Ex. 1011, Fig. 7).

Patent Owner’s arguments are not convincing because they are based on the mistaken premise that the Final Written Decision “implicitly” found that the Cloud System, Issuer System, Acquirer System, and payment network of Collinge are collectively a single remote computer system. To the contrary, the Final Written Decision states as follows:

Patent Owner further argues that for the recited “remote computer system” limitations of claim 10, Petitioner relies on a “payment network,” the “acquirer server 312,” “the issuer processing server 308,” and the “payment credentials management system,” shown as element 704, all of which, Patent Owner argues, are “not part of ‘remote SE 110.’” [PO Resp.] 32; *see also id.* at 36-37 (Patent Owner arguing that the Payment Credentials Management System is “distinct from issuer processing server 308,” and that “Petitioner presents no evidence or argument that these distinct components are part of the same remote computer system”) (citing Ex. 2009 ¶ 53).

Petitioner explains, and we agree, that Petitioner’s identification of the remote computer system of Collinge was not limited to the “remote-SE system 110,” but included other aspects of the Collinge computer system that Petitioner expressly relies upon, as shown in the annotated version of Collinge Figure 7 provided by Petitioner in Reply.⁶ Pet. Reply 16–18. We find no discrepancy in this regard with

⁶ We refer to the “annotated version of Collinge Figure 7 provided by Petitioner in Reply,” but note more specifically that in the Reply Petitioner provides an annotated version of Figure 7 from the ’095 Provisional (reproduced above), which, as explained above, Collinge incorporates by reference.

the portions of Dr. Fiske’s testimony cited by Patent Owner, which does not suggest he relied on “different” remote computer systems to meet the additional limitations of claim 10. *See* PO Resp. 30 (citing Ex. 2035: 74:15–75:9); Pet. Reply. 18.

FWD 57. Thus, contrary to Patent Owner’s allegations, the Final Written Decision finds that Petitioner has shown that the components of Collinge that Petitioner expressly relies upon as a single remote computer system correspond to the components in the “Blue-Box Structures” identified in the annotated version of Figure 7 (above) provided by Petitioner in Petitioner’s Reply, which does not include, for example, Collinge’s Acquirer System.

Next, Patent Owner argues that any determination that the components of Collinge’s system relied on by Petitioner as a “remote computer system” “would necessarily rely upon a claim construction of ‘remote computer system,’” and further asserts that we did not “directly address the scope of this term.” *Id.* at 9–10. Patent Owner purports to have raised this issue in a sentence in its Response where it argues that Collinge’s Payment Credentials Management System 704 “is distinct from issuer processing server 308,” and that “Petitioner presents no evidence or argument that these distinct components are part of the same remote computer system.” *Id.* at 10; PO Resp. 36–37.

The term “remote computer system” appears nowhere in the Specification of the ’171 patent outside of the claims. However, the ’171 patent expressly states, with additional caveats, that “the term ‘remote’ refers to locations that are geographically far apart,” and that “[o]ne indication of remoteness is that the two locations are not within a distances[sic] such that most persons at one or the other of the remote locations would consider walking to the other location, or at least would not be able to do so within one day.” Ex. 1001, 9:22–27. Thus, the

Specification addresses the spatial separation between the mobile device and a remote computer system, but does not define “computer system.”

With regard to claim construction, the Petition asserts that no express construction is necessary for any claim term and relies upon “their ordinary and customary meaning, as understood by a [person of ordinary skill in the art] at the time of the invention and in the context of the patent disclosure.” Pet. 24. Patent Owner does not dispute that Collinge teaches a “remote” computer system and does not argue that the term “computer system” is used in the ’171 patent outside of its ordinary and customary meaning. See Ex. 2009 ¶ 60 (Dr. Easttom stating in his declaration in support of Patent Owner that “throughout” his analysis he views “terms using their plain and ordinary meaning to one of ordinary skill in the art”). In the absence of any articulated dispute between the Parties, we find that “computer system” need not be expressly construed. See Ex. 1049, 25:4–6 (Dr. Fiske confirming that a person of ordinary skill in the art in 2012 would have been familiar with the term “computer system”).

Although Patent Owner characterizes its argument as based on the proper claim construction of “remote computer system,” Patent Owner’s argument is more appropriately characterized as whether the components of Collinge relied on by Petitioner are part of the *same* “remote computer system.” The elements of Collinge relied on by Petitioner in this regard are Collinge’s remote-SE system 110 and issuer processing server 308. As explained above, Petitioner establishes that remote-SE system 110 and issuer processing server 308 are part of a “remote computer system” taught in Collinge, because they are remote from the mobile device and share a communication connection, thereby forming a “system” of “computer” components, as expressly shown in Figure 7 of Collinge (and Figure 7 of the

'095 Provisional, reproduced above). Reply 17–18 (citing Ex. 1009 ¶ 46, Fig. 7). We credit Dr. Fiske in this regard, who explains that “the functionality performed” in the components in the “Blue-Box Structures,” that is Collinge’s Cloud Systema and Issuer System, “share a ‘connection 178’ therebetween,” as shown in Figure 7 of the '095 Provisional. Ex. 1050 ¶ 43.

We also considered Dr. Easttom’s opinion that Collinge’s Cloud System 110 and Issuer System 108 (see Ex. 1011, Fig. 7) are not one computer system because, in his view, each item “is (one or more) separate systems that operated independently from the others.” Ex. 2009 ¶ 150; see also PO Resp. 36–37 (arguing that Petitioner presents “no evidence” to show that allegedly “distinct” components are part of one remote computer system). We find Dr. Easttom’s opinion untenable because it is contrary to the express disclosure of Collinge, which demonstrates that, rather than operating “independently,” Cloud System 110 and Issuer System 108, and specifically remote-SE system 110 and issuer processing server 308, are connected and operate together through that connection, remotely from the mobile device. The Final Written Decision expressly agrees with and adopts Petitioner’s contentions with regard to claim 10, and we maintain that position here. See FWD 56–59.

Lastly, Patent Owner argues that Petitioner’s assertion at oral argument that the components of Collinge are “clearly working together as a system” is “an improper new argument.” DR Req. 10 n.3. Merely stating what is expressly disclosed in Collinge, i.e., that the components of Collinge relied upon by Petitioner work together, does not constitute a “new argument.” Regardless, we do not rely on counsel’s assertions at oral argument as a basis for our Decision.

3. *Dependent Claims 11–13*

Patent Owner raises no additional arguments directed to claims 11–13, which depend from claim 10, beyond the arguments addressed above in regard to claim 10. *See generally* DR Req. Our analysis and conclusions regarding claim 10 also apply to claims 11–13.

4. *Dependent Claim 27*

Patent Owner raises no additional arguments directed to claim 27, which depends from claim 17, beyond the arguments addressed above in regard to claim 10. *See generally* DR Req. To the extent Patent Owner’s arguments pertaining to claim 10 also apply to claim 27, our analysis and conclusions regarding claim 10 also apply to claim 27.⁷

5. *Dependent Claims 28–30*

Patent Owner raises no additional arguments directed to claims 28–30, which depend from claim 27, beyond the arguments addressed above in

⁷ Unlike claim 10, which refers back to “the remote computer system” of claim 1 (from which claim 10 depends), claim 27 recites “a remote computer system” and *does not* appear to refer back to “the remote computer system” of claim 17 (from which claim 27 depends). Notwithstanding this difference, Patent Owner asserts, without further explanation, that the same arguments Patent Owner raises in regard to claim 10 also apply to claim 27. DR Req. 11 (noting that Petitioner’s arguments directed to claims 10 and 27 are identical). The mere fact that Petitioner presents the same arguments for claims 10 and 27 (showing a single remote computer system taught by Collinge discloses all that is required by claims 1, 10, 17, and 27), does not mean that claim 27 *requires* a single remote computer system like claim 10 where the relevant language of claim 27 is not identical to claim 10. Accordingly, in light of the difference in claim language, we additionally find that Patent Owner offers no sufficient explanation for why its arguments premised on the relationship between “the remote computer system” of claims 1 and 10 are applicable to the recitation of “a remote computer system” in claim 17 and “a remote computer system” in claim 27.

regard to claims 10 and 27. *See generally* DR Req. Our analysis and conclusions regarding claims 10 and 27 also apply to claims 28–30.

II. CONCLUSION

For the reasons explained above, and those set forth in the Final Written Decision, Petitioner demonstrates by a preponderance of the evidence that the subject matter of claims 1–33 would have been obvious over Collinge

Our conclusions are summarized in the following table, as previously set forth in the Final Written Decision. FWD 64.

Claims	35 U.S.C. §	Reference /Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–33	103(a)	Collinge	1–33	
1–4, 6–20, 22–33	102	Collinge ⁸		
1–33	102	Fiske ⁹		
1–33	103(a)	Fiske ¹⁰		
Overall Outcome			1–33	

⁸ Because we determine that claims 1–4, 6–20, and 22–33 would have been obvious over Collinge, we do not address Petitioner’s additional arguments that claims 1–4, 6–20, 22–33 are anticipated by Collinge.

⁹ Because we determine that claims 1–33 would have been obvious over Collinge, we do not address Petitioner’s additional arguments that claims 1–33 are anticipated by Fiske.

¹⁰ Because we determine that claims 1–33 would have been obvious over Collinge, we do not address Petitioner’s additional arguments that claims 1–33 would have been obvious over Fiske.

III. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner demonstrates by a preponderance of the evidence that claims 1–33 of U.S. Patent 10,032,171 B2 are unpatentable, as addressed here and in our prior Final Written Decision; and

FURTHER ORDERED that on remand we do not disturb or modify any findings of fact or conclusions in the Final Written Decision.

IPR2023-01289
Patent 10,032,171 B2

FOR PETITIONER:

Eliot D. Williams
Jennifer Tempesta
BAKER BOTTS L.L.P
eliot.williams@bakerbotts.com
jennifer.tempesta@bakerbotts.com

For PATENT OWNER:

Seth Lindner
Brett Cooper
BC LAW GROUP, P.C.
slindner@bc-lawgroup.com
bcooper@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com