

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

U.S. Patent No. 8,886,954
IPR Case No.: IPR2024-00846

PATENT OWNER SUR-REPLY

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	CLAIM CONSTRUCTION	1
III.	TRANSACTION BETWEEN USER AND FINANCIAL MEDIA ISSUER LACKS A THIRD-PARTY TRUSTED AUTHORITY	1
IV.	THE ADVERTISING EXAMPLE FAILS TO SHOW A THIRD-PARTY TRUSTED AUTHORITY	7
V.	THE HOTEL EXAMPLE LACKS A THIRD-PARTY TRUSTED AUTHORITY	9
VI.	CONCLUSION	12

EXHIBIT LIST

No.	
2001	Claim Construction Order in <i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i> , No. 6:21-CV-00210-ADA
2002	Memo In Support of Claim Construction Order in <i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i>
2003	Markman Transcript from <i>Proxense v. Samsung Electronics, Co., Ltd. et al.</i>
2004	Claim Construction Order in <i>Proxense v. Google LLC</i> , No. 6:23-cv-00320-ADA
2005	Opening Claim Construction Brief in <i>Proxense v. Microsoft Corporation</i> , No. 6:23-cv-00319-ADA
2006	Claim Construction Order in <i>Proxense v. Microsoft Corp.</i> , No. 6:23-cv-00319- ADA
2007	Merriam-Webster Definition of Access available at https://www.merriamwebster.com/dictionary/access
2008	Chase Article on Credit Card Processing available at https://www.chase.com/personal/credit-cards/education/basics/credit-cardprocessing
2009	Stripe Statistics (2024): Revenue, Market Share & Growth Rate, https://capitaloneshopping.com/research/stripe-statistics/
2010	How Online Payment Processing Works PayPal US, https://www.paypal.com/us/brc/article/how-online-payments-processing-works
2011	How credit card processing works Stripe, https://stripe.com/en-de/resources/more/how-credit-card-transaction-processing-works-a-quick-guide
2012	How PayPal helps sellers process and accept credit card payments PayPal US, https://www.paypal.com/us/brc/article/how-paypal-works-for-sellers .
2013	Card authorization explained: How does it work? Stripe, https://stripe.com/resources/more/card-authorization-explained#what-is-card authorization .
2014	Definition of transaction PCMag, https://www.pcmag.com/encyclopedia/term/transaction

2015	Transaction Definition & Meaning - Merriam-Webster, https://www.merriam-webster.com/dictionary/transaction
2016	Microsoft Corporation's Motions for Summary Judgment in <i>Proxense v. Microsoft Corporation</i> , No. 6:23-cv-00319-ADA

I. INTRODUCTION

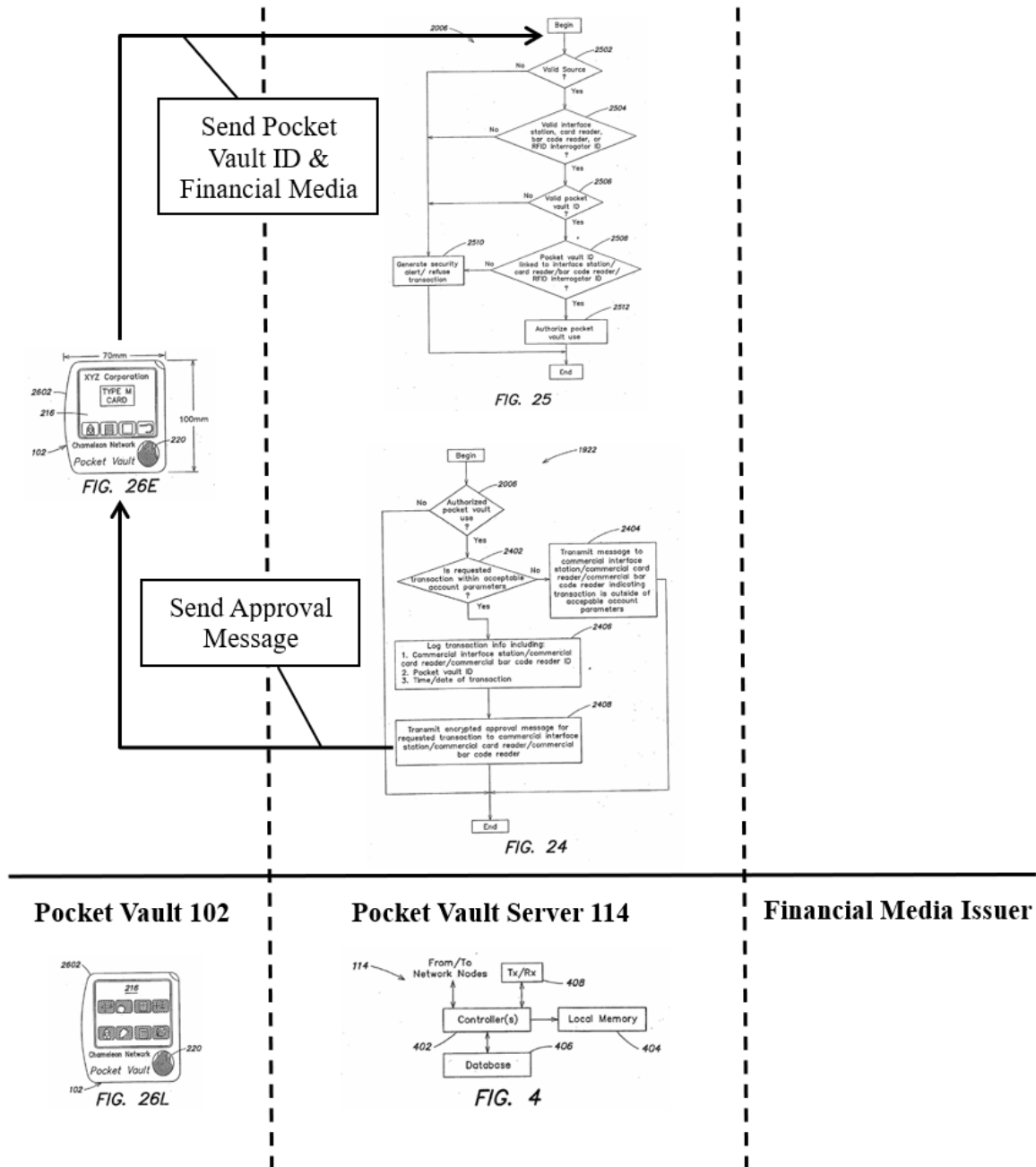
Petitioner still has not shown that the grounds of invalidity presented in the Petition demonstrate the presence of a third-party trusted authority. The clarification of the grounds of invalidity provided in Petitioner’s Reply only demonstrates the lack of a “third-party trusted authority.” First, all examples presented in the Petition involve only *two* parties – the Pocket Vault and the Pocket Vault Server. Second, Petitioner contends that a “third-party trusted authority” must be a separate entity from the application being accessed. However, the Pocket Vault Server is the application being accessed. Accordingly, under either Patent Owner’s or Petitioner’s theories, the Petition fails to show a third-party trusted authority.

II. CLAIM CONSTRUCTION

The claims at issue have been construed in *Apple Inc. v. Proxense, LLC*, IPR2024-00233, Paper 35 (PTAB June 17, 2023). Without forfeiting any right of appeal, Patent Owner believes that construction is binding upon these proceedings.

III. TRANSACTION BETWEEN USER AND FINANCIAL MEDIA ISSUER LACKS A THIRD-PARTY TRUSTED AUTHORITY

The supposed transaction between the user and financial media issuer is summarized in the below figure, which reproduces and annotates Figs. 4, 24, 25, and 26E, L of the Burger reference:



Petitioner characterizes the transaction between the user and financial media issuer as “obtaining payment information or authorization for charging a credit card or bank account.” Paper 2, at 35. Accordingly, the summary figure above reflects the

transmittal of payment information (*i.e.*, financial media issuer) from the Pocket Vault and the receipt of a transaction approval from Pocket Vault Server 114.

The second party to the transaction is supposedly the “financial media issuer 112 (*e.g.*, bank or credit card company).” *Id.* Accordingly, the summary figure also includes a column for the involvement of a financial media issuer.

Supposedly, the third-party is the “party operating the network server” 114. *Id.* The trusted authority is supposedly “the network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server.” *Id.* The summary figure also includes Pocket Vault Server 114.

According to Petitioner, “FIG. 24 [displays] the steps performed in the step(s) of processing a request to authorize a transaction of FIG. 19.” *Id.*, at 21. Additionally, the Petitioner maintains that FIG. 25 “display[s] the steps performed in the operation 2006 of authorizing use of a Pocket Vault in FIG. 24.” *Id.*, at 22. The Petitioner further maintains that “Burger’s network server implements the operations depicted in FIGS. 24 and 25.” *Id.*, at 14. Such is confirmed by Burger, which states that “[t]he local memory 404 may have instructions stored therein which, when executed by the controller 402, causes the controller 402 to implement the routines described below in connection with FIGS. 19-25 and/or FIGS. 30-39.” Burger, ¶ [0145]. Consistent with the Petitioner’s foregoing assertions and the teachings of Burger, the summary figure presents FIGS. 24 and 25 as operations of Pocket Vault Server 114.

Finally, Petitioner has not asserted that the transaction involves any actions by the Financial Media Issuer. Accordingly, the above figure has nothing in the Financial Media Issuer column, that column remains blank.

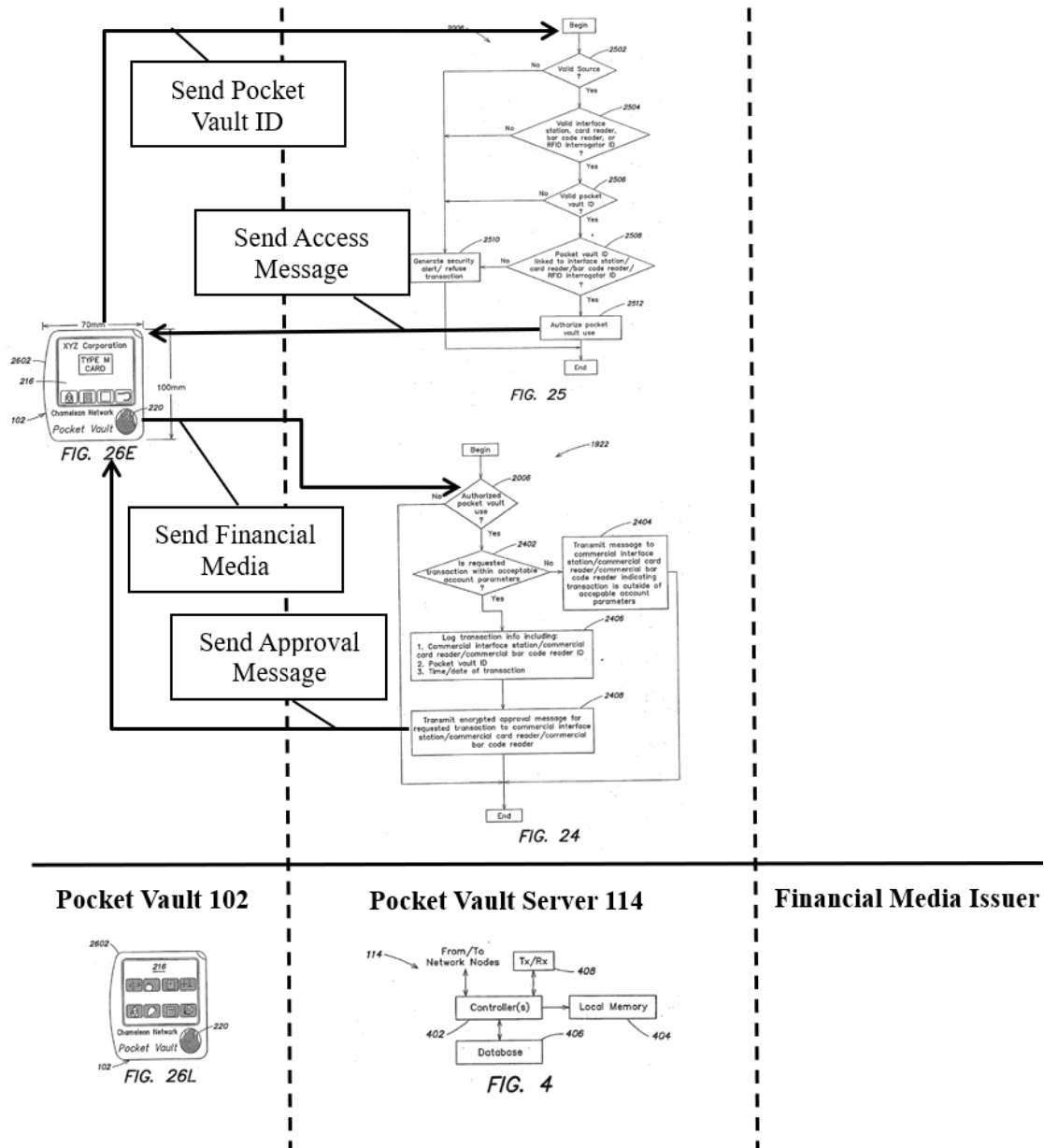
As the above demonstrates, the transaction of “obtaining payment information or authorization for charging a credit card or bank account” solely is performed by the Pocket Vault and the Pocket Vault Server 114. As the Financial Media Issuer performs no actions in the transaction, it is not a participant or party to the transaction. Consequently, the transaction is only between Pocket Vault and Pocket Vault Server 114. The transaction is thus between *two parties* – the Pocket Vault and the Pocket Vault Server 114 – and thus *lacks a third-party*.

However, the Petition asserts the claims at issue are obvious over Burger; not anticipated by Burger. Accordingly, as clarified in Petitioner’s Reply, where Petitioner quotes verbatim from the conclusory statement of its own expert:

It would have been obvious that an application in the Pocket Vault would have received an access message from the controller 402 of the network server (“receiving, at an application, an access message from the trusted authority”) *to allow users access to the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID* that was sent to the network server so that the Pocket Vault *grants access to a user and displays sensitive information (e.g., credit or debit card info) for conducting a transaction.*

Paper 14, at 11 (emphasis in original).

Such a modification of the transaction of “obtaining payment information or authorization for charging a credit card or bank account” is shown in a second summary figure below:



The only modification proposed is the Pocket Vault “receiv[ing] an access message from the controller 402 of the network server ... to allow users access to

the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID.” Petitioner characterizes the “application” being accessed as the “File or computer software (when a user is involved in a financial transaction with a retailer or credit card company).” Paper 2, at 53. Accordingly, the above figure shows: 1) sending an access message from Pocket Vault Server 114 to the Pocket Vault; and 2) sending Financial Media from the Pocket Vault to Pocket Vault Server 114.

Still, the modified transaction of “obtaining payment information or authorization for charging a credit card or bank account” is solely performed by the Pocket Vault and the Pocket Vault Server 114. As the Financial Media Issuer performs no actions in the transaction, it is not a participant or party to the modified transaction. Consequently, the modified transaction is only between Pocket Vault and Pocket Vault Server 114. The modified transaction is thus between *two parties* – the Pocket Vault and the Pocket Vault Server – and thus *lacks a third-party*.

Even if the Financial Media Issuer were involved in the transaction, the transaction would still lack a third-party. Pocket Vault and Pocket Vault Server 114 are same system. Moreover, the application being accessed, according to Burger, is still Pocket Vault Server 114. According to Petitioner, “[n]one of the expansive intrinsic evidence of the ’954 patent supports implicitly construing ‘third party’ to encompass a merely separate server controlled by the same party.” Ex 2016, at 15.

Even with Petitioner's proposed modification, for which it provides no supporting evidence, Burger discloses no server capable of providing the application being accessed (sending information from the Financial Media Issuer to the Pocket Vault device) other than Pocket Vault Server 114, which, under Petitioner's theory, also must act as the third party that operates a trusted authority. Likewise, as demonstrated above with reference to FIG. 24, "authorization for charging a credit card" is provided by the Network Server 114. Petitioner admits as much. Paper 2, Petition, at 55 ("the network server transmits an approval message for the financial transaction."); *see also id. at 20, 45* ("the controller 402 of the network server also transmits an encrypted approval message in operation 2408..."), 73 ("...the controller 202 of the Pocket Vault receives an encrypted approval message from the controller 402 of the network server..."). Accordingly, Petitioner's modification of Burger lacks a server operated by a third-party. Thus, by Petitioner's own admissions, the modified transaction of "obtaining payment information or authorization for charging a credit card or bank account" lacks a third-party.

IV. THE ADVERTISING EXAMPLE FAILS TO SHOW A THIRD-PARTY TRUSTED AUTHORITY

As detailed in Patent Owner's Response, the Advertising Example presented in the Petition lacks a separate server storing advertisements. Paper 10, at 15-20.

Burger repeatedly teaches that advertisements are stored on the Pocket Vault Server 114 and downloaded to Pocket Vaults:

“As shown in FIG. 1, the network server 114 may form the hub of the network system 100... As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.” Burger, ¶ [0098].

“[T]he network server 114 may also serve as a repository for information regarding media issuers or advertisers.” Burger, ¶ [0117].

“The advertiser 108 (FIG. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.” Burger, ¶ [0237]

“In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser.” Burger, ¶ [0538].

Thus, advertisements are stored on Pocket Vault Server 114 and downloaded to Pocket Vault software on the Pocket Vault device. Accordingly, the transaction of accessing advertisements is performed only between the Pocket Vault Server 114 and the Pocket Vault. Therefore, there are only two participants in the transaction of accessing advertisement. Consequently, to have a third-party trusted authority an

additional server would be required. Yet, the grounds of invalidity presented in the Petition fail to provide such an additional server.

Petitioner attempts to hide the missing server by stating “the application in the Pocket Value, which is what Petitioner relies upon for its prior art mapping (see Pet., 36, 39-42, 52; MSC-1005, FIG. 10) should not be conflated with software on the network server...” Paper 14, at 16. While true, this observation does not detract from the fact that Pocket Vault Server 114 is still the application being accessed as well as the purported third party that operates a trusted authority. Thus, the Advertising Example of Burger also does not show a participant other than the Pocket Vault and Pocket Vault Server 114. Accordingly, Petitioner’s observation does not provide the missing third-party. Rather, it merely confirms that the transaction is only between Pocket Vault software on a device and Pocket Vault software on a server. Thus, by Petitioner’s own admission, the Advertising Example lacks a third-party trusted authority.

V. THE HOTEL EXAMPLE LACKS A THIRD-PARTY TRUSTED AUTHORITY

As with every other example presented by Petitioner, the “Hotel Example” lacks a third-party trusted authority.

According to Petitioner, “[i]t is clear from [Burger, ¶[679] that Burger teaches that the user links with the network server 114 to download the key.” Paper 14, at 18. However, ¶ 679 of Burger does not state from where the key card is downloaded.

One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card Stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic Stripe coding to unlock the guest's hotel room.

Burger, ¶ [0679].

Nowhere does the above passage state the key card is downloaded from Pocket Vault Server 114. Even if it did, Pocket Vault Server 114 would have to be a shared drive being accessed by the Pocket Vault user. In such a situation, the Pocket Vault Server 114 would be the application (*i.e.*, the hard drive or file) being accessed. But an application cannot be a third-party unto itself. The claims clearly recite “receiving, at an application, an access message from the trusted authority ... allowing the user access to the application.” 954 Patent, Claim 1. If the application being accessed were the third-party trusted authority, it would be receiving a message from itself allowing access to itself. Such a construction would essential remove the third-party trusted authority from the claims. Accordingly, Petitioner’s interpretation of Burger’s Hotel Example necessarily lacks a server operated by a third-party.

VI. CONCLUSION

Petitioner fails to demonstrate that Burger alone or in combination with Robinson renders claims 1-29 of the 954 Patent obvious. The Petition thus fails to demonstrate the challenged claims invalid and unpatentable.

Dated: June 23, 2025

Respectfully submitted by,

/David L. Hecht/

David L. Hecht Reg. No. 61,618)

(lead counsel)

dhecht@hechtpartners.com

HECHT PARTNERS LLP

125 Park Avenue, 25th Floor

New York, NY 10017

P: (212) 851-6821

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certifies that Patent Owner Proxense, LLC's Patent Owner Sur-Reply was served on Petitioner by e-mailing copies to the e-mail addresses provided in Petitioner's Petition:

Dated: June 23, 2025

Respectfully submitted, by

/David L. Hecht/

David L Hecht

Reg. No 61,618

Hecht Partners LLP

125 Park Avenue, 25th Floor

New York, NY 10017

Tel: 212-851-6821

E: dhecht@hechtpartners.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that word count for the foregoing Patent Owner Response (excluding the table of contents, certificate of service, certificate of word count, or listing of exhibits) total 2,208 words, which is less than the 5,600 words allowed under 37 C.F.R. § 42.24(b)(4).

Dated: June 23, 2025

Respectfully submitted,

/David L. Hecht/

David L Hecht

Reg. No 61,618

Hecht Partners LLP

125 Park Avenue, 25th Floor

New York, NY 10017

Tel: 212-851-6821

E: dhecht@hechtpartners.com

Counsel for Patent Owner