

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NUVEI TECHNOLOGIES, INC.,
Petitioner,

v.

AUTOSCRIBE CORPORATION,
Patent Owner.

IPR2025-00089
Patent 11,620,621 B2

Before ST. JOHN COURTENAY III, MICHAEL R. ZECHER, and
KEVIN W. CHERRY, *Administrative Patent Judges*.

ZECHER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Petitioner, Nuvei Technologies, Inc. (“Nuvei”), filed a Petition requesting an *inter partes* review (“IPR”) of claims 1–27 of U.S. Patent No. 11,620,621 B2 (Ex. 1001, “the 621 patent”). Paper 1 (“Pet.”). Patent Owner, Autoscibe Corporation (“Autoscibe”), filed a Preliminary Response. Paper 8 (“Prelim. Resp.”). Based on the authority delegated to us by the Director under 37 C.F.R. § 42.4(a), we may not institute an IPR unless the information presented in the Petition and any preliminary response thereto shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Taking into account Autoscibe’s Preliminary Response, we conclude that the information presented in the Petition does not establish that there is a reasonable likelihood that Nuvei would prevail in challenging any one of claims 1–27 of the ’621 patent as unpatentable. We, therefore, *deny* the Petition.

A. *Real Parties in Interest (“RPIs”)*

Nuvei identifies itself, Nuvei Corporation, Nuvei Technologies Corporation, Nuvei Limited, and Nuvei International Group Limited as the RPIs. Paper 6, 1 (Nuvei’s Updated Mandatory Notices). Autoscibe identifies itself as an RPI. Paper 7, 1 (Autoscibe’s Updated Mandatory Notices).

B. *Related Matters*

The parties indicate that the ’621 patent is, or has been, asserted in the following district court cases: (1) *Autoscibe Corp. v. Repay Holdings Corp.*, No. 2:23-cv-00349 (E.D. Tex. filed July 27, 2023); (2) *Autoscibe Corp. v. Fortis Payment Sys, LLC*, No. 2:23-cv-00364 (E.D. Tex. filed Aug.

10, 2023); (3) *Autoscribe Corp. v. Payment Savvy, LLC*, No. 2:23-cv-00390 (E.D. Tex. filed Aug. 29, 2023); (4) *Autoscribe Corp. v. Tsevo, LLC*, No. 3:24-cv-00076 (S.D. Tex. filed Mar. 18, 2024); (5) *Autoscribe Corp. v. PCI Booking Ltd.*, No. 3:24-cv-00081 (S.D. Tex. filed Mar. 22, 2024); (6) *Autoscribe Corp. v. Paysafe Ltd.*, No. 3:24-cv-00104 (S.D. Tex. filed Apr. 11, 2024); (7) *Autoscribe Corp. v. Nuvei Corp.*, No. 2:24-cv-00325 (E.D. Tex. filed May 3, 2024); and (8) *Autoscribe Corp. v. M&A Ventures, LLC*, No. 1:24-cv-04282-SCJ (N.D. GA. filed Sep 24, 2024). Paper 6, 1; Paper 7, 1.

In addition to this Petition, M&A Ventures, LLC, Replay Holdings Corporation and Repay Holdings, LLC (collectively, “M&A Ventures”) filed another petition challenging the same claims of the ’621 patent. *M&A Ventures, LLC v. Autoscribe Corp.*, IPR2024-01159, Paper 1 (PTAB July 18, 2024) (Petition challenging claims 1–27 of the ’621 patent). We denied institution of M&A Ventures’s Petition. *M&A Ventures, LLC v. Autoscribe Corp.*, IPR2024-01159, Paper 12 (PTAB Jan. 29, 2025) (Decision Denying Institution).

C. The ’621 Patent

The ’621 patent, titled “Enrolling a Payer by a Merchant Server Operated by or for the Benefit of a Payee and Processing a Payment from the Payer by a Secure Server,” issued from U.S. Patent Application No. 16/535,424 (“the ’424 application”), filed on August 8, 2019. Ex. 1001, codes (54), (21), (22). The ’621 patent is a continuation of U.S. Patent Application No. 15/408,185, which issued as U.S. Patent No. 10,423,940 B2, which, in turn, is a continuation of U.S. Patent Application No. 13/679,545, which issued as U.S. Patent No. 9,576,279 B2 (“the ’279

patent”). *Id.* at code (63). The ’621 patent ultimately has a claim of priority to U.S. Provisional Patent Application No. 61/655,482 (“the ’482 application”), which was filed on June 5, 2012. *Id.* at code (60).

The ’621 patent generally relates to “systems and methods for obtaining and using account information to process financial payments.” Ex. 1001,1:18–20. The ’621 patent states that, “[i]n the payments industry, tokenization has become a popular means of bolstering the security of electronic transactions while minimizing the complexity of compliance with industry standards and best practices.” *Id.* at 1:59–62. The ’621 patent, however, states that “[t]here is a need for improvement in conventional approaches to obtaining and using account information to process financial payments” due to the “limits in functionality of existing tokenization methods.” *Id.* at 2:4–7.

The ’621 patent purportedly addresses this need by establishing a “customer (payer) enrollment session” wherein the enrollment session is initiated by a merchant server where the customer provides information relevant to the enrollment session, but the session itself is completed on a secure server that may be different from the merchant server. Ex. 1001, 2:19–35. The secure server “stores the financial account information received from the customer” and “provides a token to the merchant’s server.” *Id.* at 2:51–54. The operator of the secure server may process the payment using the financial account pointed by the token and make the proceeds available to the merchant. *Id.* at 3:6–9.

Figure 3 of the '621 patent, reproduced below, illustrates “a method of registering customer financial information and processing payments” in accordance with one embodiment. Ex. 1001, 3:30–31.

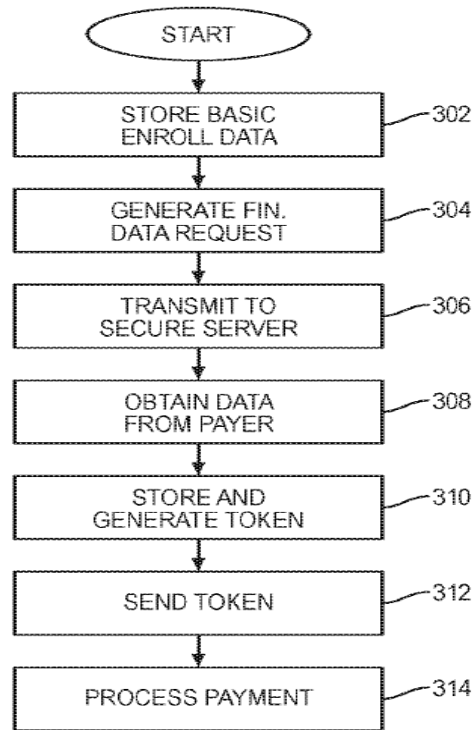


FIG. 3

Figure 3 illustrates a “general method and process for enrolling a payer in an electronic system and then making a payment based on the enrollment.” *Id.* at 7:50–54. The method begins at step 302 where “enrollment data identifying a payer” is stored in a first computing system. *Id.* at 7:53–55. At step 304, the first computing system (e.g., a merchant server) generates an “electronic instruction to a second computing system” to “obtain financial account information from the payer.” *Id.* at 7:65–8:2. At step 306, this instruction is transmitted to the second computing system. *Id.* at 8:23–24. At step 308, the second computing system communicates with the payer, during which the payer can “provide the sensitive financial account

information to the second computing system without this information being visible . . . by the operator of the first computing system.” *Id.* at 8:32–35.

Next, at step 310, the financial account information is stored in the second computing system and a token is generated for the referring payee (e.g., a merchant server). Ex. 1001, 8:37–40. The token is “a pointer that allows the payee to reference the financial account information of that payer without possessing the actual financial account information.” *Id.* at 8:40–43. Then, at step 312, “the first computing system receives the token from the second computing system in response to its instruction to obtain financial account information for the payer.” *Id.* at 8:44–66. According to the ‘621 patent, this “completes the registration of the payer so as to enable one or more intended payments to the payee using the stored financial account information.” *Id.* at 8:49–51. At step 314, once registration is complete, the payee can “process an authorized payment from the payer by electronically generating a payment transaction instruction in the first computing system” and “electronically transmitting the payment transaction instruction to a computing system other than the first computing system.” *Id.* at 8:52–59.

D. Challenged Claims

Of the challenged claims, claims 1, 8, 15, 23, and 25 are independent. Independent claim 1 is directed to “[a] method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers,” independent claim 8 is directed to “[a] secure server that processes a payment transaction from a payer to a payee,” independent claim 15 is directed to “[a] method of enrolling a payer by a merchant server operated by or for the benefit of a payee,” independent claim 23 is directed to “[a] merchant server, operated by or for the benefit of a payee,” and

independent claim 25 is directed to “[a] method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers.” Ex. 1001, 16:53–55, 18:20–21, 19:60–62, 21:4–5, 22:1–3. Claims 2–7 directly or indirectly depend from independent claim 1, claims 9–14 directly or indirectly depend from independent claim 8, claims 16–22 directly depend from independent claim 15, claim 24 directly depends from independent claim 23, and claims 26 and 27 directly depend from claim 25. *Id.* at 17:58–18:19, 19:30–59, 20:49–21:3, 21:65–67, 23:1–6. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers, the method comprising:

providing, by the one or more secure servers to a merchant server providing a webpage to a payer computing system used by the payer, an application programming interface (API) that:

provides financial account registration and token retrieval functions that can be executed to process the payment transaction;

provides access to the financial account registration and token retrieval functions to the merchant server;

receives, from the merchant server via the API, at least one data element associated with the payer and a payment amount from the payer to the payee;

authenticates the payee; and

executes the financial account registration function, upon initiation by the merchant server, by:

generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

establishing the secure socket layer connection, in response to an HTTP request received from the merchant server for the generated URL, between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server via the secure socket layer connection;

receiving the sensitive financial account information provided by the payer via the secure socket layer connection;

storing the sensitive financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

executing a token retrieval function, upon initiation by the merchant server via the API, by:

providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant server without providing the sensitive financial account information to the merchant server and *without providing the non-sensitive electronic data token to the payer*; and

processing the payment transaction using the sensitive financial account information by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

Id. at 16:53–17:57 (emphasis added).

E. Asserted Prior Art References

Nuvei relies on the prior art references set forth in the tables below.

Name¹	Reference	Dates	Exhibit No.
Stringfellow	U.S. Patent Application Publication No. 2010/0174626 A1	published July 8, 2010; filed Apr. 1, 2009	1007
Kloster	U.S. Patent Application Publication No. 2010/0094755 A1	published Apr. 15, 2010; filed Oct. 9, 2009	1008
Carlson	U.S. Patent No. 8,606,700 B2	issued Dec. 10, 2013; filed Jan. 25, 2012	1018

F. Asserted Grounds of Unpatentability

Nuvei challenges claims 1–27 of the ’621 patent based on the asserted grounds of unpatentability set forth in the table below. Pet. 8–9, 20–72.

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–27	103(a) ²	Stringfellow, Kloster
1–27	103(a)	Stringfellow, Kloster, Carlson

¹ For clarity and ease of reference, we only list the first named inventor.

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the ’621 patent claims the benefit of the ’482 application, which was filed before this date, the pre-AIA version of § 103 applies. Ex. 1001, codes (21), (22), (60), (63).

II. ANALYSIS

A. Claim Construction

In this IPR, claim terms are construed using the same claim construction standard as in a civil action under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b). That is, claim terms generally are construed in accordance with their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art, in view of the specification and the prosecution history pertaining to the patent at issue. *See id.* The ordinary and customary meaning of a claim term “is its meaning to the ordinary artisan after reading the entire patent,” and “as of the effective filing date of the patent application.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 1321 (Fed. Cir. 2005) (en banc).

In the Petition, Nuvei proposes that claim construction is unnecessary to resolve the dispute between the parties, and each claim term should be given its plain and ordinary meaning. Pet. 18. In the Preliminary Response, Autoscribe does not identify any particular claim term that requires construction. *See* Prelim. Resp.

Based on the preliminary record, there is no readily discernible controversy between the parties that requires us to construe any claim terms at this time. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

B. Obviousness Over the Combined Teachings of Stringfellow and Kloster

Nuvei contends that claims 1–27 of the ’621 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Stringfellow and Kloster. Pet. 20–70. Nuvei contends that the combined teachings of Stringfellow and Kloster account for the subject matter of each challenged claim, and provides reasoning as to why a person of ordinary skill in the art would have been prompted to combine the relevant teachings. *Id.* Nuvei submits the testimony of Kevin C. Almeroth, Ph.D. to support its positions. *See* Ex. 1005.

Based on the preliminary record, we determine that Nuvei has not shown that there is a reasonable likelihood that it would prevail in challenging any of the claims of the ’621 patent as unpatentable. We begin our analysis with the principles of law that generally apply to an asserted ground based on obviousness, followed by an assessment of the level of skill in the art, next we provide overviews of Stringfellow and Kloster, and then we address the parties’ contentions with respect to the independent claims 1, 8, 15, 23, and 25.

1. Principles of Law

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, “would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in

the art; and (4) when in evidence, objective indicia of obviousness or non-obviousness (i.e., secondary considerations, such as commercial success, long-felt but unsolved needs, failure of others, etc.).³ *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966). We analyze the asserted grounds based on obviousness with the principles we identify above in mind.

2. *Level of Skill in the Art*

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The “person having ordinary skill in the art” is a hypothetical construct, from whose vantage point obviousness is assessed. *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998).

Factors pertinent to a determination of the level of ordinary skill in the art include “(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field.” *Env’t Designs, Ltd. v. Union Oil Co. of Cal.*, 713 F.2d 693, 696 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). “Not all such factors may be present in every case, and

³ At this stage in the proceeding, Autoscribe does not present arguments or evidence of secondary considerations. See Prelim. Resp.

one or more of these or other factors may predominate in a particular case.”
Id. at 696–97.

In the Petition, Nuvei contends that a person having ordinary skill in the art “would have had at least (1) an undergraduate degree in electrical engineering, computer engineering, computer science, or comparable field of study, and (2) at least two years’ experience working with and programming networked computer systems.” Pet. 9 (citing Ex. 1005 ¶ 36). Nuvei also argues that “[a]dditional education might substitute for some experience, and vice versa.” *Id.* In the Preliminary Response, Autoscribe does not address the level of skill in the art. *See* Prelim. Resp.

Accordingly, for purposes of this Decision, we adopt Nuvei’s proposed assessment of the level of ordinary skill in the art because it is consistent with both the ’621 patent and the asserted prior art, and it is supported by the testimony of Dr. Almeroth.

3. Overview of Stringfellow

Stringfellow generally relates to “a method of processing payment [authorization] requests for payment transactions.” Ex. 1007, code (57). In particular, the disclosed method is conducted by a trusted central intermediary system that is configured to transmit payment authorization requests to a plurality of online merchant Internet Payment Service Provider (“IPSP”) systems. *Id.*

Figure 3 of Stringfellow, reproduced below, illustrates the flow of data during use of a payment system. Ex. 1007 ¶¶ 33, 45.

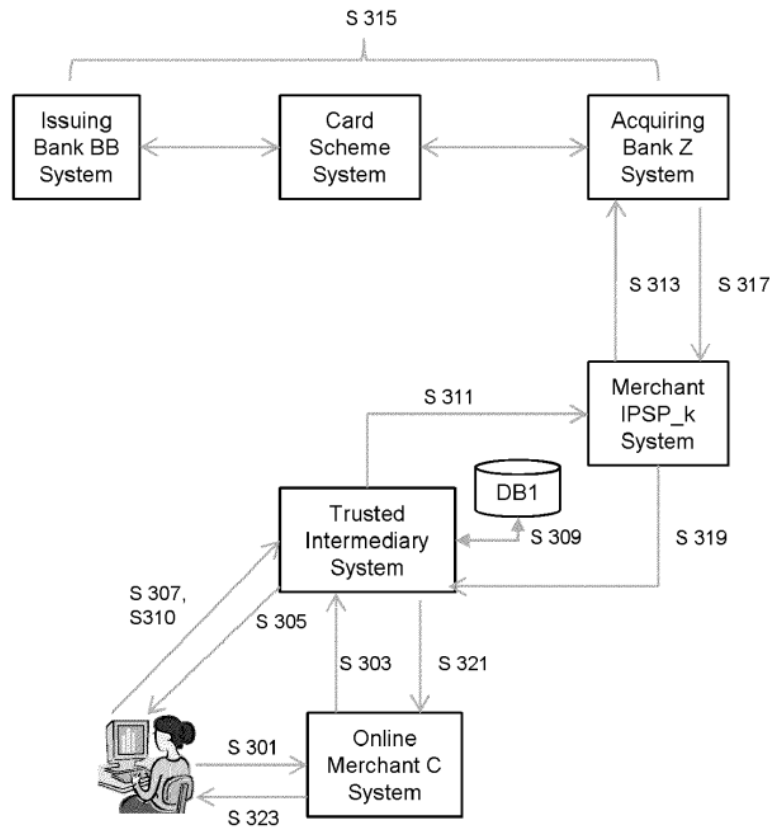


Figure 3 illustrates how a user (initially being on the merchant’s website) completes his/her shopping experience with online merchant C’s system, and initiates a virtual checkout by selecting “Secure System for Payment” (“SSP”) as a payment option (step S301). *Id.* ¶ 45. Selecting SSP as a payment option causes the online merchant C’s system to transmit an originating payment authorization request to the trusted intermediary system (step S303). *Id.* The trusted intermediary system then transmits a login uniform resource locator (“URL”) to the user (step S305), prompting the user to login (step S307), or, if this is the first time the user selects SSP as a payment option, the user may register with the trusted intermediary system. *Id.*; *see also id.* ¶¶ 53–56 (describing different ways by which a user may register with the trusted intermediary system service). The trusted

intermediary system then performs a lookup based on the user's credentials and identifications (step S309) by retrieving details regarding the user's stored payment information from database DB1. *Id.* ¶ 46. Upon selection of the desired stored payment method, the trusted intermediary system sends a payment authorization request to the online merchant's IPSP system (step S311), which, in turn, sends a further authorization request to the acquiring bank (step S313). *Id.* Once the acquiring bank authorizes payment, the online merchant's IPSP system and the trusted intermediary system work together to process a payment confirmation notification (steps S319, S321), at which point the online merchant C's system confirms the order status with the user (step S323). *Id.* ¶¶ 46, 47.

4. Overview of Kloster

Kloster is generally directed to “providing an inline frame (iFrame) and secure cross domain messaging for collecting sensitive payment data.” Ex. 1008, code (57). In particular, Kloster discloses associating a payment data token with the sensitive payment data collected through the inline frame. *Id.*

Figure 1 of Kloster, reproduced below, illustrates a system for implementing the disclosed method. Ex. 1008 ¶ 8.

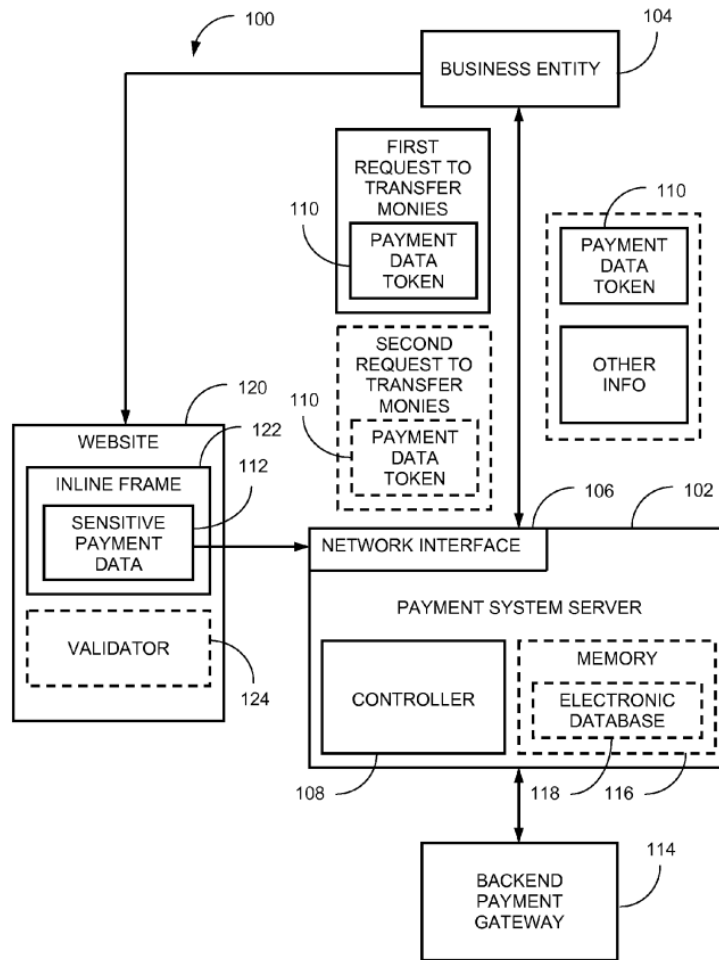


Figure 1 illustrates business entity 104 that hosts website 120 for selling goods/services, with payment system server 102 providing the business entity with one or more inline frames 122 that can be hosted directly on website 120. *Id.* ¶ 16. In addition, each inline frame 122 is configured to communicate directly with payment system server 102, such that the customer may enter and submit confidential information. *Id.* According to Kloster, by embedding inline frame 122 directly within website 120 of business entity 104, payment system server 102 is able to receive sensitive

payment data 112 from an end user without requiring business entity 104 to collect sensitive payment data 112. *Id.*

Figure 2 of Kloster, reproduced below, further illustrates the particular method steps in a flow diagram. Ex. 1008 ¶ 9.

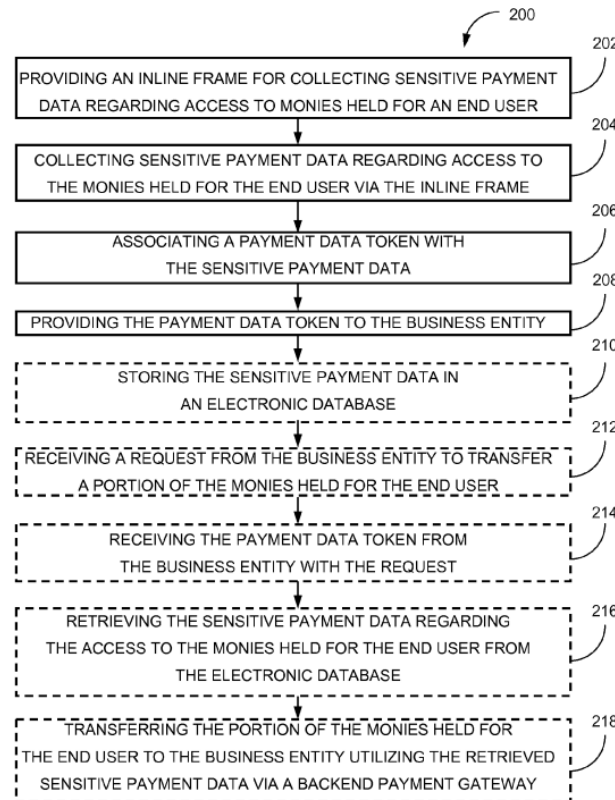


Figure 2 illustrates, among other things, that after collecting the sensitive payment data, Kloster discloses associating a payment data token⁴ with the sensitive payment data (step 206). *Id.* ¶ 23. Next, Kloster discloses providing the payment data token to the business entity (step 208). *Id.* In particular, Kloster discloses one example where, “in a specific

⁴ According to Kloster “a payment data token is a system generated identifier comprised of a string of characters that may be utilized as a key to refer to sensitive payment data.” Ex. 1008 ¶ 13. Kloster discloses that these payment data tokens “only ha[ve] meaning within the payment system” and “could not be used to process payments at physical merchant locations.” *Id.*

implementation of secure cross domain messaging, the inline frame may be redirected to a call back URL.” *Id.* ¶ 23. Kloster builds on this example by disclosing that “the payment data token is passed as a parameter to the call back URL.” *Id.*

Once the business entity receives the payment data token and stores it within an electronic database (steps 210, 214), the business entity sends a request to the payment system server to transfer at least a portion of the monies held for the end user to the business entity. Ex. 1008 ¶¶ 23, 24. Thereafter, the payment system server transfers a portion of monies held for the end user through a backend payment gateway (step 218), where the gateway may respond indicating success or failure regarding the transaction. *Id.* ¶ 24.

5. Claims 1, 8, 15, 23, and 25

Nuvei contends that the combined teachings of Stringfellow and Kloster account for all of the limitations of independent claims 1, 8, 15, 23, 25. Pet. 36–53, 57–60, 62–69. Of particular importance to this asserted obviousness ground is Nuvei’s reliance on Kloster to meet a negative limitation that is recited in each independent claim. Pet. 51–52, 60, 63, 67, 69. Independent claims 1, 8, and 25 each recite, in relevant part, “providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant server . . . *without providing the non-sensitive electronic data token to the payer.*” Ex. 1001, 17:46–51 (claim 1), 19:17–22 (claim 8), 22:56–61 (claim 25) (emphasis added). Independent claim 15 recites, in relevant part, “receiving the non-sensitive data token from the secure server, wherein . . . the secure server *does not provide the non-sensitive electronic data token to the payer.*” *Id.* at 20:33–38 (emphasis

added). Similar to independent claim 15, independent claim 23 recites, in relevant part, that the merchant server is programmed to “receive the non-sensitive electronic data token from the secure server, . . . and *the secure server does not provide the non-sensitive electronic data token to the payer.*” *Id.* at 21:47–52 (emphasis added). For purposes of our analysis, we group these limitations together given the substantial similarity in claim language (hereinafter known as the “without providing” negative limitation).

To satisfy this “without providing” negative limitation, Nuvei contends that Kloster’s token retrieval disclosures where “the payment data token is passed as a parameter to the call back URL” or, alternatively, “could be retrieved” through “API calls by the merchant,” teaches the “without providing” negative limitation because the payment data token is a “system generated identifier” used to “refer to sensitive payment” that “only has meaning within the payment system.” Pet.50–51 (emphasis omitted) (quoting Ex. 1008 ¶¶ 13, 15, 23) (citing Ex. 1008 ¶¶ 4, 21, 24, 25; Ex. 1005 ¶ 100). Nuvei argues that “Kloster discloses the online merchant . . . using the token exclusively as part of direct communications with the trusted intermediary system.” *Id.* at 51 (citing Ex. 1008 ¶¶ 24, 26; Ex. 1005 ¶ 100). According to Nuvei, because Kloster “does not disclose providing the token to the payer nor any application of the use of the token that involves the payer,” a person of ordinary skill in the art would have understood that it would, at a minimum, be obvious “to not provide the data token to the payer because doing so would serve no purpose and would jeopardize security[□] by unnecessarily exposing a token that can be used to request payments.” *Id.* at 51–52 (footnote omitted) (citing Ex. 1005 ¶ 100).

In addition, Nuvei contends that, “to the extent Kloster’s disclosure of a passing a payment data token as a parameter to the call back URL that redirects an ‘iframe’ provided by the online merchant system is interpreted as the token being sent from the trusted intermediary system to the payer computer system, such functionality is still sufficient to meet the [‘without providing’]” negative claim limitation, “which precludes providing the token to the payer (i.e., the user), not the separately-recited payer computer system.” Pet. 52 n.4 (citing Ex. 1005 ¶ 100).

Nuvei relies on essentially the same arguments and evidence discussed above with respect to the “without providing” negative limitation of independent claim 1 to explain how the combined teachings of Stringfellow and Kloster account for the similar negative limitations required by independent claims 8, 15, 23, and 25. *See* Pet. 60 (limitation [8.2.1.8.1]), 63 (limitation [15.8]), 67 (limitation [23.2.8]), 69 (limitation [25.4.1]).

In the Preliminary Response, Autoscribe contends that Kloster does not teach the “without providing” negative limitation because Kloster sends the payment data token to the payer. Prelim. Resp. 44–45. In particular, Autoscribe argues that Kloster’s payment data token is sent to the payer as a parameter to the call back URL:

In one example of secure cross-domain messaging, the business entity 104 may provide the payment system server 102 with a call back Uniform Resource Locator (URL), and the payment system server 102 may pass the payment data token 110 as a parameter to the call back URL.

[...]

The payment data token is provided to the business entity, [step] 208. (The sensitive payment data may be stored in an electronic

database, [step] 210). For instance, in a specific implementation of secure cross domain messaging, the inline frame may be redirected to a call back URL specified by the merchant. In a specific example, the URL is in the same domain as the original payment page. Continuing the present example, the payment data token is passed as a parameter to the call back URL.

Id. ¶ 45 (emphasis omitted) (quoting Ex. 1008 ¶¶ 15, 23). Stated differently, Autoscribe asserts that, because Kloster’s secure server appends the payment data token as a hypertext markup language (“HTML”) parameter to the call back URL to which the secure server redirects the payer’s browser within the inline frame, it cannot teach the “without providing” negative limitation of independent claim 1. *Id.*

Based on the preliminary record, we agree with Autoscribe’s argument that Kloster does not teach the “without providing” negative limitation required by each independent claim. Nuvei appears to contend that Kloster teaches this limitation in two different ways—namely, through either a “call back URL” or “API calls by the merchant.” Pet. 50–51 (emphasis omitted) (quoting Ex. 1008 ¶¶ 15, 23) (citing Ex. 1008 ¶ 24). We address Nuvei’s contentions in turn.

First, when according the “without providing” negative limitation its plain and ordinary meaning, Kloster’s token retrieval disclosure where “the payment data token is passed as a parameter to the call back URL” results in sending the payment data token. Ex. 1008 ¶¶ 15, 23, 24. Because Kloster includes the payment data token as a parameter to the call back URL within the inline frame provided by the online merchant system (*id.* ¶¶ 15, 23), Kloster provides the payment data token to the payer and, therefore, violates this negative limitation.

We do not agree with Nuvei’s contention that a person of ordinary skill in the art would have understood that, from reading Kloster, the payment data token is not provided to the payer because doing so would raise security concerns. *See* Pet. 51–52 (citing Ex. 1005 ¶ 100). As we discuss above, Kloster discloses providing the payment data token to the payer by including the token within the call back URL within the inline frame provided by the online merchant system. Ex. 1008 ¶¶ 15, 23, 24. Nuvei does not direct us to, nor can we find, disclosures in Kloster teaching or suggesting that including the payment data token, which “only has meaning within the payment system,” within a call back URL would present a cognizable threat such that a person of ordinary skill in the art would not provide the payment data token to the payer. *Id.* ¶ 13.

In addition, we do not agree with Nuvei’s attempt to distinguish between providing Kloster’s payment data token to a payer computer system and providing the payment data token to a payer. *See* Pet. 52 n.4. In our view, this is a distinction without a difference. The relevant disclosures in Kloster ground the different embodiments, including the payer’s perspective, in the use of a payer computer system. *See, e.g.,* Ex. 1008 ¶¶ 11 (disclosing “system 100 and . . . method 200 for allowing an online merchant to accept payments over a computer network (e.g., the Internet)”), 12 (disclosing “network interface 106 may be utilized to receive a request to transfer monies from an end user (customer) to . . . business entity 104”), 22 (disclosing that “an end user (customer) connects to the online merchant’s website and navigates to a payment page”).

With this in mind, Kloster’s disclosure of providing the data token to the payer computer system is effectively the same as providing it to the

payer, who is operating the payer computer system. This reading of Kloster also is consistent with how the ‘621 patent blurs the lines between the payer and the payer computer system. *See, e.g.*, Ex. 1001 9:55–59 (disclosing that “Internet[,] Merchant server 204 may provide the customer at site 206, 208 or 210 with a widget or redirected URL that provides an online window”).

Second, there is insufficient evidentiary support to determine whether, during Kloster’s “API calls by the merchant,” the payment data token is not sent to the payer when performing token retrieval functions. Ex. 1008 ¶ 15. Merely demonstrating that Kloster is silent regarding providing the payment data token to the payer during API calls made by the merchant, without more evidence regarding what a person of ordinary skill in the art would have understood from reading Kloster, is insufficient to show that the token is not provided to the payer because “[s]ilence is generally not disclosure.” *Cf. Novartis Pharms. Corp. v. Accord Healthcare, Inc.*, 38 F.4th 1013, 1017 (Fed. Cir. 2022), *cert. denied sub nom. Novartis Pharms. Corp. v. HEC Pharm Co.*, 143 S. Ct. 1748 (Mem) (2023).

The U.S. Court of Appeals for the Federal Circuit has held that a reference’s silence, standing alone, is not sufficient to demonstrate the absence of a feature (i.e., whether a reference teaches or suggests a negative limitation). *See In re Strongbridge Dublin Ltd.*, Nos. 2023-2302, 2023-2303, 2025 WL 751116 at *4 (Fed. Cir. Mar. 10, 2025) (“There must be something more to suggest that the silence is significant, or other reasons that establish . . . it is likely that one or more of the patients in Sansone **were not taking** famotidine or methotrexate at some time during the nine week and/or fifty-two-week length of the study.” (emphasis added)); *see also IBM*

Corp. v. Iancu, 759 F. App'x 1002, 1011 (Fed. Cir. 2019) (explaining that a reference's silence is inadequate proof of a negative limitation's disclosure).

We are, however, mindful that “a reference need not state a feature's absence in order to disclose a negative limitation.” *AC Techs. S.A. v. Amazon.com, Inc.*, 912 F.3d 1358, 1367 (Fed. Cir. 2019); *see Almirall, LLC v. Amneal Pharms. LLC*, 28 F.4th 265, 273 (Fed. Cir. 2022) (“[I]t was reasonable for the Board to find that, in the context of [a prior art reference], a skilled artisan would recognize that the reference discloses a complete formulation—**excluding** the possibility of an additional active ingredient.” (emphasis added)). “In determining what a prior art reference discloses, we look to what a skilled artisan would understand from reading the reference, which includes the internal context within the reference.” *United Servs. Automobile Assoc. v. PNC Bank N.A.*, No. 2023-2244, 2025 WL 706080, at *3 (Fed. Cir. Mar. 5, 2025). Here, Kloster clearly discloses providing the payment data token to the payer by including the token within the call back URL within the inline frame provided by the online merchant system (*see* Ex. 1008 ¶ 23), and Kloster does not identify any other disadvantages associated with providing the payment data token to the payer that would bear on our reading of API calls made by the merchant (*see id.* ¶ 15).

The supporting testimony from Nuvei's declarant, Dr. Almeroth, on these issues fare no better. Dr. Almeroth provides no additional explanation beyond the arguments and evidence presented in the Petition to support Nuvei's assertion that Kloster does not provide the payment data token to the payer during its token retrieval functions. *See* Ex. 1005 ¶ 100.

For all the reasons we identify above, Nuvei does not present sufficient evidence to support a finding that Kloster teaches the “without

providing” negative limitation of independent claim 1, and the similar negative limitations of independent claims 8, 15, 23, and 25. Accordingly, Nuvei has not shown a reasonable likelihood that it would prevail on its assertions that the subject matter of independent claims 1, 8, 15, 23, and 25 would have been obvious over the combined teachings of Stringfellow and Kloster.

6. Claims 2–7, 9–14, 16–22, 24, 26, and 27

By virtue of their dependency, claims 2–7, 9–14, 16–22, 24, 26, and 27 include the same limitations as at least one of independent claim 1, 8, 15, 23 or 25. Nuvei does not present arguments or evidence with respect to these dependent claims that remedy the deficiencies in its obviousness analysis of independent claims 1, 8, 15, 23 and 25. *See* Pet. 53–56, 60–61, 65–66, 68, 70. Accordingly, Nuvei has not shown a reasonable likelihood that it would prevail on its assertions that the subject matter of dependent claims 2–7, 9–14, 16–22, 24, 26, and 27 would have been obvious over the combined teachings of Stringfellow and Kloster.

C. Obviousness Over the Combined Teachings of Stringfellow, Kloster and Carlson

Nuvei contends that claims 1–27 of the ’621 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Stringfellow, Kloster, and Carlson. Pet. 70–72. With a few exceptions, Nuvei relies on essentially the same arguments and evidence it identifies above with respect to independent claims 1, 8, 15, 23, and 25 to support its asserted obviousness ground based on the combined teachings of Stringfellow, Kloster, and Carlson challenging these same claims. *Id.* at 72. As applied by Nuvei, Carlson does not remedy the deficiencies in the

combined teachings of Stringfellow and Kloster that we identify above. *See id.* at 70–72. Accordingly, Nuvei has not shown a reasonable likelihood that it would prevail on its assertions that the subject matter of claims 1–27 would have been obvious over the combined teachings of Stringfellow, Kloster, and Carlson.

III. CONCLUSION

Taking into account Autoscribe’s Preliminary Response, we conclude that the information presented in the Petition does not demonstrate that there is a reasonable likelihood that Nuvei would prevail in challenging any one of claims 1–27 of the ’621 patent as unpatentable.

IV. ORDER

In consideration of the foregoing, it is ORDERED that the Petition is *denied* and no trial is instituted.

IPR2025-00089
Patent 11,620,621 B2

FOR PETITION:

Eagle Robinson
Daniel Leventhal
NORTON ROSE FULBRIGHT US LLP
eagle.robinson@nortonrosefulbright.com,
daniel.leventhal@nortonrosefulbright.com

FOR PATENT OWNER:

Sujeeth Rajavolu
AHMAD ZAVITSANOS & MENSING PLLC
sujeeth.rajavolu@gmail.com