

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Askeladden L.L.C.,
Petitioner

v.

Calabrese Stemer LLC,
Patent Owner

Case: IPR2024-00369
U.S. Patent No. 7,954,706

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Mandatory Notices.	1
A.	Real Party-in-Interest.	1
B.	Related Matters.	1
C.	Fee.	1
D.	Designation of Lead and Backup Counsel.	2
E.	Service Information.	2
II.	Introduction.	4
III.	The '706 Patent.	4
A.	Prosecution of the '706 patent.	7
B.	Level of Ordinary Skill in the Art.	7
IV.	Claim Construction.	8
V.	Relief Requested.	9
A.	Grounds for Standing.	9
B.	Identification of Challenge	9
VI.	Prior Art.	10
A.	Horie (Ex. 1006)	10
B.	Kobayashi (Ex. 1007)	12
C.	Kano (Ex. 1011).	16
VII.	Motivations to Modify and/or Combine References.	17
A.	Motivation to Combine Horie with Kobayashi.	18
VIII.	Full Statement of the Reasons for the Relief Requested.	21
A.	GROUND 1: Claims 1-2 should be cancelled as anticipated by Horie.	21
1.	Independent claim 1.	22
2.	Dependent claim 2 – The method according to claim 1, wherein authorization request includes the account information and a monetary amount, and the notification to the communications device associated with the customer in an SMS message including the monetary amount.	28

B. GROUND 2: Claims 1-2 should be cancelled as obvious by Horie and the knowledge of a POSITA.	30
1. Independent claim 1.	30
2. Dependent claim 2 – The method according to claim 1, wherein authorization request includes the account information and a monetary amount, and the notification to the communications device associated with the customer in an SMS message including the monetary amount.	31
C. GROUND 3: Claims 3-5 should be cancelled as obvious by Horie in view of Kobayashi.	32
1. Dependent claim 3 – The method according to claim 1, which further comprises prompting the customer to return a response to the notification and authorizing the purchase only when a proper response is returned.	32
2. Dependent claim 4 – The method according to claim 3, wherein the response includes a personal identifier associated with the customer.	35
3. Independent claim 5.	36
D. GROUND 4: Claims 6-7 should be cancelled as anticipated by Kano.	46
1. Independent claim 6.	46
2. Dependent claim 7 – The method according to claim 6, wherein the preauthorization from the customer includes a maximum amount to be authorized for the transaction and a time period within which the preauthorization is valid.	56
E. GROUND 5: Claims 6-7 should be cancelled as obvious by Kano and the knowledge of a POSITA.	57
1. Independent claim 6.	57
2. Dependent claim 7 – The method according to claim 6, wherein the preauthorization from the customer includes a maximum amount to be authorized for the transaction and a time period within which the preauthorization is valid.	58
IX. Denial Under § 325(d) is Inappropriate.	59
X. Discretionary Denial is Inappropriate.	59
XI. Conclusion.	59

LIST OF EXHIBITS

PETITIONER EXHIBIT	DESCRIPTION
1001	U.S. Patent No. 7,954,706 (“the ’706 patent”)
1002	Prosecution History of the ’706 patent
1003	Declaration and <i>curriculum vitae</i> of Dr. Robert Akl, D. Sc.
1004	Declaration of Glenn J. Perry
1005	Supporting Exhibit to Declaration of Glenn J. Perry
1006	Certified English Translation of Japanese Patent Application No. 2002-133100 (“Horie”) and Certification
1007	Certified English Translation of Japanese Patent Application No. 2001-306806 (“Kobayashi”) and Certification
1008	U.S. Patent No. 5,915,222 (“the ’222 patent”)
1009	Japanese Patent Application No. 2002-133100 (“Horie”)
1010	Japanese Patent Application No. 2001-306806 (“Kobayashi”)
1011	Certified English Translation of Patent Cooperation Treaty No. WO 2002-008981 (“Kano”) and Certification
1012	Patent Cooperation Treaty No. WO 2002-008981 (“Kano”)
1013	Prosecution History of the ’310 patent

CLAIM LISTING

Claim 1
[1pre] 1. A payment authorization method, which comprises:
[1a] gathering, at a merchant's, account information for payment of a customer's purchase;
[1b] transmitting an authorization request from the merchant's to a financial authorization system requesting payment authorization for the customer's purchase;
[1c] checking whether or not a profile is present with regard to the customer and, if the profile is present, checking whether or not the customer has requested notification regarding the authorization request;
[1d] if the customer has requested notification, notifying the customer that the authorization request has been received by transmitting a notification to a cell phone or a cellular network-connected communications device associated with the customer; and
[1e] processing the transaction for payment authorization and, if the purchase is authorized, notifying the merchant substantially contemporaneously with the step of transmitting the notification to the cell phone or the communications device associated with the customer.
Claim 2
2. The method according to claim 1, wherein the authorization request includes the account information and a monetary amount, and the notification to the communications device associated with the customer in an SMS message including the monetary amount.
Claim 3
3. The method according to claim 1, which further comprises prompting the customer to return a response to the notification and authorizing the purchase only when a proper response is returned.

Claim 4
4. The method according to claim 3, wherein the response includes a personal identifier associated with the customer.
Claim 5
[5pre] 1. A charge card processing method, which comprises:
[5a] inputting a transaction request to a stationary merchant terminal disposed at a merchant location;
[5b] processing the transaction request with the merchant terminal, including a transmission of a first authorization request to a remote processing facility and receipt of a notification that authorization has been accepted or declined;
[5c] transmitting a second authorization request from a remote processing facility to a mobile communications device of a customer associated with the requested transaction through a cellular network; and
[5d] authorizing the requested transaction only if authorization has been accepted for the first authorization request and a proper response has been received by the remote processing facility to the second authorization request.
Claim 6
[6pre] 1. A charge card processing method, which comprises:
[6a] preauthorizing an imminent given transaction by transmitting a preauthorization for the imminent given transaction from a customer to a financial authorization system;
[6b] subsequently inputting a transaction request concerning the given transaction at a merchant terminal disposed at a merchant location;
[6c] processing the transaction request at the merchant terminal, including a transmission of an authorization request for the given transaction to the financial authorization system;
[6d] transmitting a response to the authorization request from the financial authorization system to the merchant terminal, and thereby authorizing the transaction request at the merchant's if the preauthorization from the customer is available in the financial authorization system, and otherwise contacting the

customer for authorization or declining the authorization request.

Claim 7

7. The method according to claim 6, wherein the preauthorization from the customer includes a maximum amount to be authorized for the transaction and a time period within which the preauthorization is valid.

I. Mandatory Notices.

A. Real Party-in-Interest.

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner Askeladden L.L.C. certifies that it is the real party-in-interest in this proceeding. In this regard, Petitioner submits the Declaration of Glenn J. Perry (Ex. 1004) and supporting exhibit (Ex. 1005). As demonstrated in the Perry Declaration and supporting exhibit, no other party is in privity with or exercised control or could exercise control over Petitioner's participation in this proceeding, the filing of this Petition, or the conduct of any ensuing trial. Ex. 1004 ¶¶22-28; Ex. 1005.

B. Related Matters.

There are no lawsuits or PTAB proceedings Petitioner is aware of involving U.S. Patent No. 7,954,706 ("the '706 patent"). To the best of Petitioner's knowledge, none of the grounds set forth in this Petition have been previously considered by the USPTO or any court. Concurrently with the filing of this Petition, Petitioner is submitting Petitions for *inter partes* review of two related patents, U.S. Patent Nos. 7,357,310 and 8,783,564.

C. Fee.

This Petition requests review of seven (7) claims of the '706 patent and is accompanied by a payment of \$41,500, which includes the \$19,000 *inter partes* review request fee, and the \$22,500 post-institution fee. *See* 37 C.F.R. § 42.15.

Thus, this Petition meets the fee requirements under 35 U.S.C. § 312(a)(1). The Board is hereby authorized to charge any additional fees required by this action to Deposit Account No. 20-1430.

D. Designation of Lead and Backup Counsel.

Lead counsel for Petitioner is Alton L. Absher III, Registration No. 60,687 of Kilpatrick Townsend & Stockton LLP. Back-up counsel for Petitioner is Andrew W. Rinehart, Registration No. 75,537, and Philip E. Hawkyard, Registration No. 81,629, also of Kilpatrick Townsend & Stockton LLP.

<u>Lead Counsel</u>	
Alton L. Absher (Reg. No. 60,687) 1001 West Fourth Street Winston-Salem, NC 27101 Office: 336.607.7307 Fax: 336.734.2755 aabsher@ktslaw.com	

<u>Backup Counsel</u>	
Andrew W. Rinehart (Reg. No. 75,537) 1001 West Fourth Street Winston-Salem, NC 27101 Office: 336.607.7312 Fax: 336.607.7500 ARinehart@ktslaw.com	Philip E. Hawkyard (Reg. No. 81,629) Two Embarcadero Center, Suite 1900 San Francisco, CA 94111 Office: 415.273.7589 Fax: 650.618.2711 phawkyard@ktslaw.com

E. Service Information.

Petitioner may be served via email to its counsel and to

[Askeladden_IPR@ktslaw.com.](mailto:Askeladden_IPR@ktslaw.com)

II. Introduction.

The '706 patent is invalid. The only alleged points of novelty in the '706 patent—simultaneously authorizing a card transaction and notifying a card holder of the transaction via text if the customer account included a request for notification thereof and providing a preauthorization card transaction method—were already known in the art. The dependent claims of the '706 patent recite nothing more than a customer authorizing a purchase that are typical of every card transaction, and thus were well within the knowledge of a POSITA at the time of invention. All claims of the '706 patent should be cancelled as anticipated or obvious.

III. The '706 Patent.

The '706 patent was filed on March 6, 2008, as U.S. Serial No. 12/043,235 (“the '235 Application”) and issued on June 7, 2011. The '235 Application is a divisional of U.S. Serial No. 11/077,783, filed on March 11, 2005, and which was granted as U.S. Patent No. 7,357,310 B2. For the purposes of this Petition, Askeladden assumes that the earliest potential effective filing date is March 11, 2005. Because its earliest effective filing date is before March 16, 2013, the '706 patent is subject to the pre-AIA provisions of 35 U.S.C. *See* AIA § 3(n)(1).

The '706 patent, titled “Mobile Phone Charge Card Notification and Authorization Method,” generally describes “a non-intrusive, user-selectable

notification and authorization system for credit card transactions.” Ex. 1001, at 1:52-53. The method begins when a customer “swipe[s]” or “manually enter[s]” a “charge card” at a “merchant terminal.” *Id.* at 3:24-25. According to the patent, the merchant terminal can be either “a store, . . . a teller or an automated teller machine (ATM), or . . . a virtual terminal in an internet-type transaction.” *Id.* at 3:26-28.

According to the ’706 patent, “[c]redit cards and charge cards have become the primary vehicle by which payments . . . are transacted” but “charge errors and charge fraud causes millions of dollars in losses in the United States.” *Id.* at 1:21-22, 39-41. These errors occur, according to the patent, when the consumer is “charged too much” or “authorize[s] the incorrect amount,” but more often errors occur when there are “incorrect or non-authorized charges” related to “fraudulent or even innocent mistakes.” *Id.* at 1:29-30, 36-38. The patent proposes that these errors “could have been avoided, had better authorization security been assured” during the time of purchase. *Id.* at 1:38-39.

Before the customer signs for the purchase, the “merchant terminal 3 connects, through a modem 5, to an acquirer 6” and the acquirer “checks against its data sources whether or not the transaction should be authorized.” *Id.* at 3:34-38. At the same time, the acquirer also checks “the customer’s set preferences concerning the notification/authorization options.” *Id.* at 3:38-40. The customer’s

profile can be “set to simple ‘notification,’ which means the system only notifies the cardholder by sending a message to his wireless device.” *Id.* at 3:42-44.

Alternatively, the profile may require a “prompt [to the customer] to confirm the purchase.” *Id.* at 3:50-51

The patent asserts that this notification/authorization method “does not add any time to the transaction” but that any “delay” may be justified by “[t]he added security.” *Id.* at 3:60-64. However, any delay can be avoided if the customer “provide[s] preauthorization when a charge request is imminent” by “call[ing] ‘ahead’ and provid[ing] preauthorization for the impending purchase.” *Id.* at 3:66-4:3. (marked up to show “first authentication request” in red, “second authorization request” in orange, “merchant”/“merchant terminal” in green, “notification” in purple, and “preauthorization” in light blue).

Figures 1 and 2 of the ’706 patent are reproduced below.

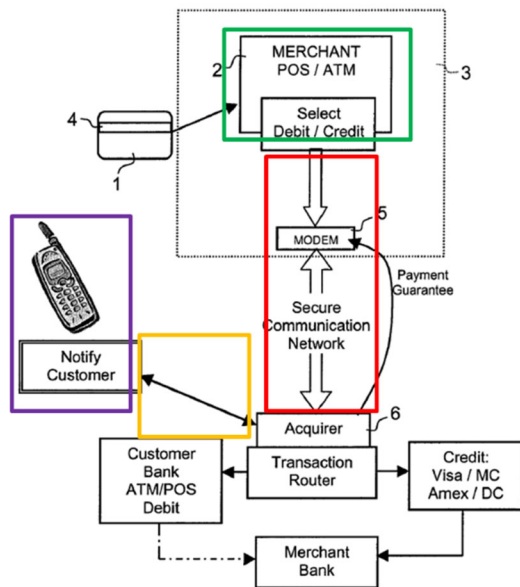


FIG. 1

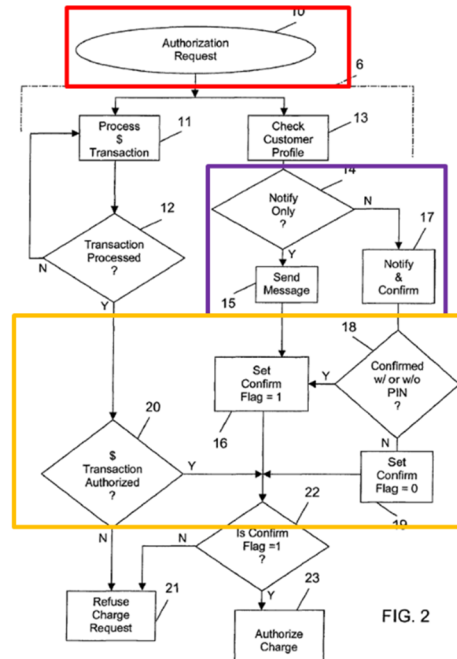


FIG. 2

Ex. 1001, Figs. 1 and 2 (annotated).

A. Prosecution of the '706 patent.

The allowed claims of the '706 patent were never rejected during prosecution by the Examiner. In a non-final rejection dated November 5, 2010, the Examiner allowed original claims 1-4 and 8-10, and rejected claims 5-7. Ex. 1002, at 117. Following an Amendment and an Examiner's Interview dated, the applicant cancelled claims 5-7. *Id.* at 134. A Notice of Allowance for the allowed claims issued on January 21, 2011. *Id.* at 140.

B. Level of Ordinary Skill in the Art.

A POSITA of the '706 patent ("POSITA") would generally have experience in the hardware and software used in the field of securely transmitting and processing authorization requests over wired and wireless networks, such as

requests for the processing of financial transactions. Ex. 1003 ¶ 22. A POSITA in this context would have a bachelor's degree in computer science, computer engineering, electrical engineering, or a related study, and would have at least one or two years of experience with wired and wireless networks used to securely process requests for authorization of activity such as financial transactions. *Id.* Less experience is necessary with additional education (e.g., a Master's degree), and likewise, less education is necessary with additional work experience (e.g., 5-6 years). *Id.*

IV. Claim Construction.

At this stage of the proceedings, Petitioner respectfully submits that no claim terms require an express construction. Ex. 1003 ¶ 62. However, independent claim 1 of the '706 patent recites a or the "merchant's." *See, e.g.*, claim 1[a] ("gathering, at a merchant's, account information..."). Based on the applicant's statements during prosecution of a related patent, U.S. 7,357,310, Petitioner submits that instances of "[a/the] merchant's" in the challenged claims of the '706 patent refer to a merchant's *terminal*. For example, during prosecution of U.S. 7,357,310, the applicant explained that the "secure network and the 'payment guarantee' channel are illustrated between the acquirer 8 [*sic*] and the modem 5 of the merchant's *terminal*." Ex. 1013, at 45 (emphasis added). While Petitioner respectfully submits that no express construction is necessary, Petitioner provides

this clarification of the claim language based on the applicant's statements. Ex. 1003 ¶ 63.

V. Relief Requested

A. Grounds for Standing

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '706 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified.

B. Identification of Challenge

Pursuant to 37 C.F.R. § 42.104(b) and 35 U.S.C. § 311, this Petition requests cancellation of claims 1-7 ("the challenged claims") of the '706 patent based on the following prior art references:

- Japanese Patent Application 2002-133100 ("the '100 application" or "Horie") [Ex. 1006];
- Japanese Patent Application 2001-306806 ("the '806 application" or "Kobayashi") [Ex. 1007].
- Patent Cooperation Treaty Patent Application WO 2002/008981 ("the '981 application" or "Kano") [Ex. 1011].

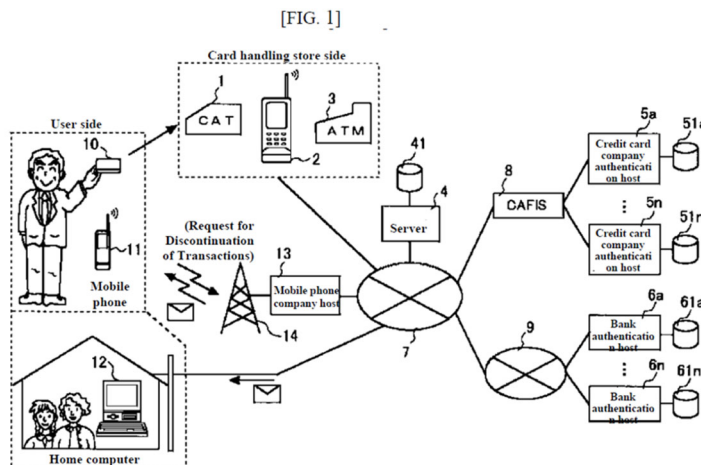
Ground	35 U.S.C.	Claims	References
1	§ 102	1-2	Horie
2	§ 103	1-2	Horie and the knowledge of a POSITA
3	§ 103	3-5	Horie in view of Kobayashi
4	§ 102	6-7	Kano
5	§ 103	6-7	Kano and the knowledge of a POSITA

VI. Prior Art

A. Horie (Ex. 1006)

Horie was published on May 10, 2002, and is therefore prior art under pre-AIA 35 U.S.C. § 102(b). Horie was not cited during prosecution of the '706 patent. Horie discloses “a card usage status notification method that **automatically notifies** a card user [] that a card payment transaction has occurred . . . using an informational terminal device such as a mobile phone or a personal computer” Ex. 1006, at [0001].

Figure 1 depicts “a schematic configuration of the entire card payment transaction system” *Id.* at [0075].



Ex. 1006, Fig. 1.

As shown, the method “has a card transaction terminal device . . . , an information processing company server 4, a credit card company authentication host 5 for card authentication processing when using a credit card, a bank authentication host 6 for card authentication processing when using a debit card (cash card), a network 7 connecting them, [and] a mobile phone company host 13 . . .” *Id.* at [0076]. According to Horie, “when there is a card payment transaction, a processing request for card usage status notification from the side of the card authentication host 5 to 6 is received at the server 4 once . . . and a processing request is sent from the side of the server 4 to the host of the applicable mobile phone company to make such a notification.” *Id.* at [0077].

In one embodiment of Horie, “the special processing for notification is continued until the specific signal and/or specific data is sent from the mobile phone company host 13 to the mobile phone 11.” *Id.* at [0078]. In this way, “various preset incoming behavior patterns” such as “an incoming melody, vibration in manner mode, [or] lighting of a light” “allow the mobile phone user to know that a particular card has been used for a payment transaction.” *Id.* at [0079]. Further, “specific data indicating the content of card payment transactions can be transmitted from the mobile phone company host to a mobile phone 12, and the mobile phone 12 can display the content on the display by text, etc.” *Id.*

Horie discloses as a goal “to provide a card usage status notification method that more quickly and reliably notifies a user to that effect, thereby enabling detection of card fraud” *Id.* at [0006]. Therefore, “a father who wants to keep track of the credit card usage status of his wife and children at all times can find out more quickly and reliably without notification from his family.” *Id.* at [0013].

Horie discloses “card[s]” which can include “a credit card, a debit card” as well as “various payment transaction cards such as cash advance cards issued by consumer financial institutions.” *Id.* at [0009]. A “card payment transaction,” as described by Horie, includes “product purchases, cash advance services, deposits and withdrawals to and from bank accounts, and the like.” *Id.*

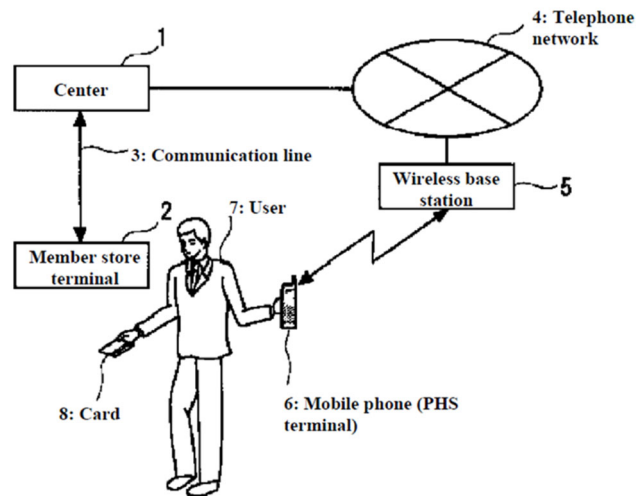
Finally, according to Horie, “when using card payment transactions, both normal card authentication processing and card usage status notification . . . are performed simultaneously.” *Id.* at [0043].

B. Kobayashi (Ex. 1007)

Kobayashi was published on November 2, 2001, and is therefore prior art under pre-AIA 35 U.S.C. § 102(b). Kobayashi was not cited during prosecution of the '706 patent. Kobayashi discloses “a card usage status notification method that automatically notifies a card user [] that a card payment transaction has occurred . . . using an informational terminal device such as a mobile phone or a personal computer” Ex. 1007, at [0001].

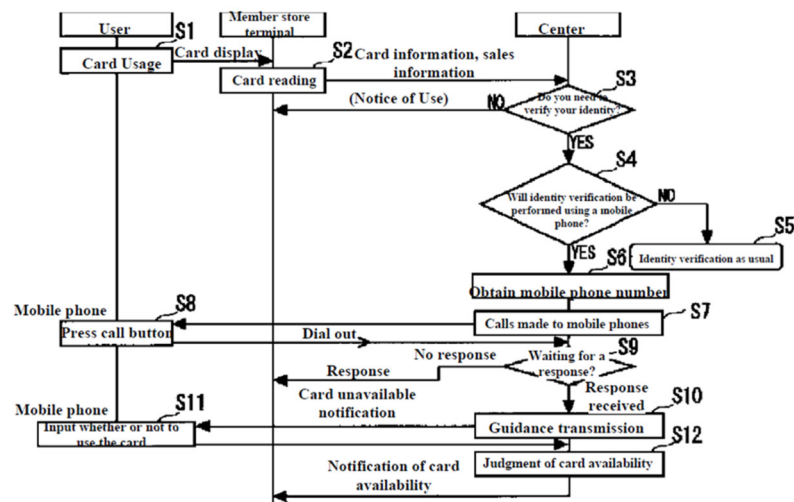
Fig. 1 is “a diagram showing a system configuration of the present invention.” *Id.* at [0040]. Figure 4 is a diagram that explains “the processing flow of the user 7 (mobile phone 6), member store terminal 2, and center 1 in one embodiment of the present invention.” *Id.* at [0053].

[FIG. 1]



Ex. 1007, Fig. 1.

[FIG. 4]



Ex. 1007, Fig. 4.

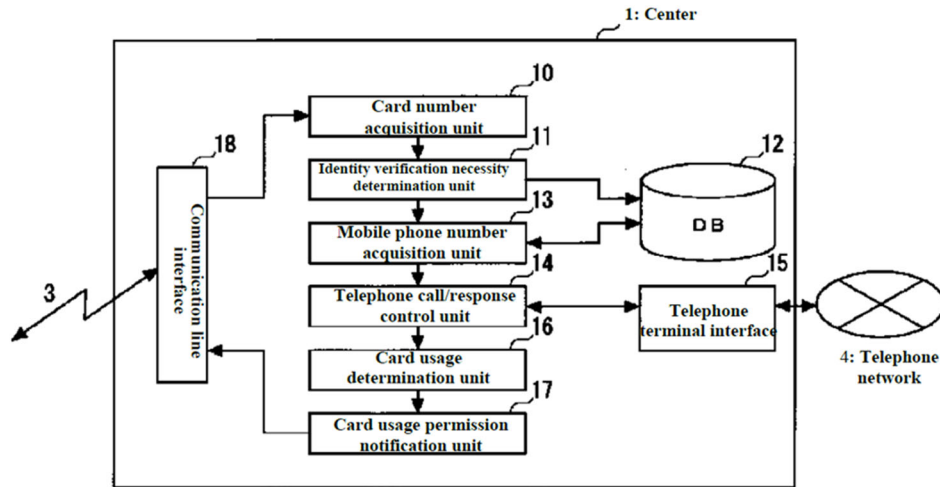
According to Kobayashi, the method includes “a member store terminal 2 having a credit card reader, and a center 1 of a credit card company which is connected to the member store terminal 2 via a communication line 3 and performs card management.” *Id.* at [0040]. “When a user 7 uses a card for payment at the time of purchasing a product at a card member store . . . the card information and sales information are transmitted from the member store terminal 2 to the center 1 via [a] communication line 3.” *Id.* at [0042].

The center will then “retrieve[] the telephone number of the portable telephone set of the user registered in advance from the card number transmitted from the member store terminal 2 and makes a call to the portable telephone set 6 of the user.” *Id.* at [0043]. Then if “the user makes a speech connection in response to the incoming call notice . . . that the card can be used . . . the use of the card is enabled.” *Id.* at [0044].

Figure 2 shows a process for determining whether to seek user authorization by the center. The center “includes a database 12 in which a mobile phone number, a password, and the like of a member are registered as member information in association with a card number (ID) for each member.” *Id.* at [0047]. When the center receives card information, it will “search[] a database 12 from the card number, and confirm[] whether or not a mode for performing

principal confirmation by a cellular phone is set from record data corresponding to the card number.” *Id.*

[FIG. 2]



Ex. 1007, Fig. 2.

According to the invention, “[w]hen a portable telephone set 6 . . . responds to a call from a center 1 . . . and card usable information is inputted” then the card is made usable. *Id.* at [0048]. However, when the user provides “information indicating that the card cannot be used” or “when the mobile phone 6 does not respond to a call from the mobile phone 6” then the card is set to “be unavailable.” *Id.* at [0049].

The user, “[a]t the time of creating the card” will describe in the application form “whether or not to perform identity verification using a mobile phone” and the “telephone number and password of the mobile phone owned by the user.” *Id.* at [0050].

C. Kano (Ex. 1011)

Kano was published on January 31, 2002, and is therefore prior art under pre-AIA 35 U.S.C. § 102(b). Kano was not cited during prosecution of the '706 patent. Kano discloses “a commercial transaction method, device, and system that can authenticate [a] person without disclosing confidential data such as credit numbers to a person authentication institution or credit card company, and can safely settle the purchase of goods.” Ex. 1011, 7:39-42.

In the purchasing method of Kano, the customer will set his/her mobile phone “to the mobile shopping mode” and then enters information related to the purchase he/she wishes to make including “the store ID,” “his or her personal ID number,” “the payment method,” and “the purchase price of the product.” *Id.* at 13:33-37. The information inputted by the user “is sent to the authentication server” for an authorization request and the authentication server “performs authentication processing for the store and the user.” *Id.* at 13:47-49. The authentication server will verify that “the store ID is registered,” “the user with the PIN number and the credit card number . . . is registered,” and the “usage limit or the balance” of the user’s input. *Id.* at 13:50-14:8. Based on these verifications, “a transaction prohibition message or QR authorized certification key is generated” and “transmitted to the mobile phone.” *Id.* at 14:9-14.

If the transaction is approved, “a QR authorized certification key consisting

of a two-dimensional code . . . is generated . . . and transmitted to the mobile phone.” *Id.* at 14:12-14. The user then “presents the pre-selected desired product to the store staff,” “places an order for the desired product,” and “inserts and attaches the mobile phone 1 with the QR authorized key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22.” *Id.* at 14:20-24. Finally, if the QR code “is recognized as genuine” then “the authentication server 41 returns the detailed settlement approval to the store terminal 22.” *Id.* at 14:49-50.

VII. Motivations to Modify and/or Combine References

A combination of familiar elements according to known methods which yields no more than predictable results is likely obvious to one of skill in the art. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). One rationale to support a conclusion of obviousness is the use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR*, 550 U.S. at 417-18; *see also* MPEP 2143(C). To establish that a modification is the use of a known technique to improve similar devices and methods in the same way, it is necessary to establish (1) that the prior art contained a “base” device/method upon which the claimed invention can be seen as an “improvement,” (2) a finding that the prior art contained a “comparable” device/method that is not the same as the base device/method and that has been improved in the same way as the claimed

invention, and (3) that the skilled artisan could have applied the known “improvement” technique in the same way to the base device/method with predictable results. *See* MPEP 2143(C); *KSR*, 550 U.S. at 415-421.

A. Motivation to Combine Horie with Kobayashi.

A POSITA would have been motivated to combine the disclosures of Horie and Kobayashi at the time of the alleged invention of the ’706 patent. Ex. 1003 ¶ 66. Horie and Kobayashi both describe the same field of technology: systems and methods for commercial transaction settlement. *See, e.g.*, Ex. 1006, Abstract (“a card payment transaction system that enables online card payment transactions”); Ex. 1007, [0001] (“a method, system, and recording medium suitable for preventing unauthorized use of cards such as credit cards used by card members for product payment, financing, etc.”); Ex. 1003 ¶ 67. Furthermore, both references describe the use of similar hardware, such as mobile phones, wired and wireless networks, credit / ATM cards, and point-of-sale payment processors. *Compare* Ex. 1006, Figs. 1, 9 *with* Ex. 1007, Figs. 1, 7-10; Ex. 1003 ¶ 68. In addition, both Horie and Kobayashi are directed to systems and methods to monitor credit card usage and prevent unauthorized transactions. Ex. 1006, Abstract (“a card authentication host is provided with a means to create an email to notify the user of a card payment transaction”); Ex. 1007, Summary (“a method and system that can confirm the user's identity when the user uses a card and

prevent unauthorized use by a third party.”); Ex. 1003 ¶¶ 69-70. At least for these reasons, a POSITA would have considered these references to be analogous art. *See In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992); Ex. 1003 ¶ 71.

Horie also discloses the use of transaction notifications sent to a user’s mobile device for the purpose of preventing illegal card use or fraud. *See* Ex. 1006, [0073]. However, while Horie specifically describes that “it would be possible to prevent fraudulent card use by making it possible to issue a transaction cancellation request to the authentication hosts 5 to 6 via the mobile phone 11,” Horie fails to disclose any further details on how to issue a transaction cancellation request through a mobile phone. *Id.*; Ex. 1003 ¶ 72.

Absent this detail, a POSITA seeking to implement the system described in Horie would have looked to known techniques for preventing fraudulent transactions / credit fraud via a mobile device, such as what is disclosed in Kobayashi. Ex. 1003 ¶ 73. Kobayashi, for example, discloses “a mode in which identity verification is performed by a mobile phone, the phone number of the mobile phone registered corresponding to the card number is searched and obtained from database 12 (step S6), and the phone number of the mobile phone is automatically dialed (step S7).” Ex. 1007, [0057]; Ex. 1003 ¶ 74. According to Kobayashi, the “user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step S11). The input

information indicating whether the card can be used or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.” Ex. 1007, [0060]. Based on that input information, the “center 1 judges the card usage permission information transmitted from the mobile phone 6, determines whether the card can be used (step S12), and notifies the member store terminal 2 of the determination result of the usage permission.” Ex. 1007, [0061]; Ex. 1003 ¶ 74.

Because Horie and Kobayashi are within the same technological field and describe the use of the same types of hardware to achieve similar results, a POSITA would have considered the use of Kobayashi’s fraud prevention interface to be an improvement on the system described in Horie, which itself does not provide any technical details on how to issue a transaction stop request through a mobile phone. Ex. 1003 ¶ 75. A POSITA would have found this implementation to be a straightforward combination of prior art elements and the use of a known technique (Kobayashi) to improve a similar system (Horie) in the same way. Ex. 1003 ¶ 75. Given the similar technology and hardware described in both references, a POSITA would have had a reasonable expectation of success in combining these disclosures. Ex. 1003 ¶ 76. The use of Kobayashi’s input information to provide card usage authorization by a customer from the customer’s mobile phone would have been nothing more than a predictable use of known

mobile technology according to its established function of sending and receiving data via a cellular or wireless network. *See KSR*, 550 U.S. at 417; Ex. 1003 ¶ 76.

Furthermore, a POSITA would have been motivated and encouraged to combine these references in this manner because Kobayashi describes an efficient method for processing a transaction stop request using known hardware that would have been inexpensive to implement in the system described in Horie without requiring, for example, modifications to the hardware and system architecture already described and implemented in Horie. Ex. 1003 ¶ 76. A POSITA would have seen Kobayashi's input information as an improvement to the system disclosed in Horie because Horie does not describe any implementation details of how to issue a "transaction cancellation request to the authentication host," and Kobayashi describes an efficient, simple solution for that feature that would have been possible without any changes to the hardware of the mobile device described in Horie. Ex. 1003 ¶ 76.

VIII. Full Statement of the Reasons for the Relief Requested.

A. GROUND 1: Claims 1-2 should be cancelled as anticipated by Horie.

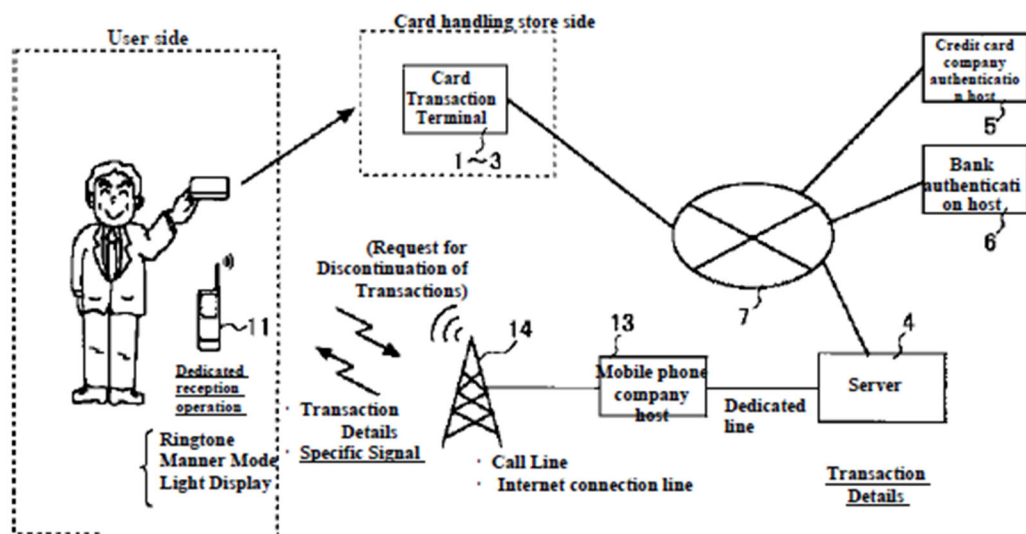
Horie discloses each element of claims 1 and 2 and therefore anticipates each challenged claim 1 and 2 ("Ground 1").

1. Independent claim 1.

i. Preamble – A payment authorization method, which comprises:

To the extent the preamble is limiting, it is disclosed by Horie. Horie “relates to a card usage status notification method that automatically notifies a card user, etc. that a card payment transaction has occurred via a network, and a card payment transaction system using the same method.” Ex. 1006, at [0001]; Ex. 1003 ¶ 127.

The method of Horie is shown in Figure 9, below:



Ex. 1006, Fig. 9.

ii. Element [1a] – gathering, at a merchant's, account information for payment of a customer's purchase;

Horie discloses this limitation. Horie discloses that “when the [card authorization] process is started, card information, transaction details information, and other necessary information are sequentially read on the card transaction

terminal device side (steps 201, 202, and 203).” Ex. 1006, [0046]. Further, Horie discloses that the “card information includes card number information.” *Id.* at [0047]. Horie further discloses that “when card 10 owned by a card user is used for payment transactions via **card transaction terminal devices 1 to 3**, card authentication processing is performed between card transaction terminal devices 1 to 3 and each authentication host” *Id.* at [0044]. Horie defines “**card transaction terminal device**” as including “**CAT (wireless CAT etc. may also be used), ATM, Kiosk terminal device, etc.**” *Id.* at [0025]. Horie further discloses that the “card transaction terminal device[s] . . . [are] installed on the card handling store side.” *Id.* at [0076]. Horie further explains that a CAT, which can be installed at a “card handling store” for a “product purchase.” *Id.*, at [0039], [0047]. Thus, the account information is gathered “at a merchant’s.”

Therefore, Horie discloses this limitation because the card transaction terminal devices, which are “installed on the card handling store side” (i.e., the merchant store), “read” the “card information,” including “the card number information.” Ex. 1003 ¶ 129.

iii. Element [1b] – transmitting an **authorization request from the **merchant’s** to a financial authorization system requesting payment authorization for the customer’s purchase**

Horie discloses this limitation. Horie discloses that “[t]he various types of information that have been read are sent as data to each card authentication host 5-

6 (or CAFIS 8), **thereby issuing a card authentication processing request** (step 204).” Ex. 1006, [0048]; Ex. 1003 ¶ 131. Horie further discloses that “when the [card authorization] process is started, card information, transaction details information, and other necessary information are sequentially read on the **card transaction terminal device side** (steps 201, 202, and 203).” Horie, [0046]. Horie states that “[t]he authentication process is then performed based on the received information (step 304)” and that the “card authentication process is actually executed via the CAFIS 8.” *Id.* at [0054]; Ex. 1003 ¶¶ 132-133. Therefore, Horie discloses that the information gathered at the merchant’s terminal device is sent to CAFIS 8 (or a related authentication host), and that CAFIS / authentication host itself actually executes the card authentication and authorization. Ex. 1003 ¶ 134.

iv. *Element [1c]* – checking whether or not a profile is present with regard to the customer and, if the profile is present, checking whether or not the customer has requested **notification regarding the authorization request;**

Horie discloses this limitation. Horie discloses that during the transaction “a **predetermined file is called for determining whether or not to notify the user of the card payment transaction**” Ex. 1006, at [0057]; Ex. 1003 ¶ 135. Horie further discloses that “[i]f the email notification service is not requested here (step 310 NO), the processing is terminated. That is, in this case, a normal card payment transaction is performed as usual and the process ends. On the other hand, if the email notification service has been applied for (step 310 YES), **a request for email**

transmission processing is made to the server 4 via the network 7 (step 311). That is, in this example, processing for sending e-mail is performed on the server 4 side.” *Id.* at [0059]; Ex. 1003 ¶ 136.

Horie further discloses that “when creating a card, the user must indicate on the application form whether or not to use a mobile phone to verify their identity, and if they wish to use a mobile phone to verify their identity, the telephone number and password of the mobile possessed by the user are recorded in the database 12, and the telephone number of the mobile phone and, if necessary, the password are also associated with the card number (ID) and registered in the database 12.” *Id.* at [0050]. Horie further discloses that “[c]ardholders who already have a card can receive the service of the system according to the invention by simply notifying the card company of the mobile phone number owned by the cardholder, and there is no need to issue a new card.” *Id.* at [0051]; Ex. 1003 ¶ 137.

Thus, Horie discloses the limitation because during card creation, or for those who already own a card, the card holder indicates whether or not they wish to be notified during transactions. Ex. 1003 ¶ 138. This information is added to a “predetermined file” (i.e., the customer’s profile), and the “predetermined file” is then checked to determine whether or not to notify the customer. Ex. 1003 ¶ 138.

- v. ***Element [1d]* – if the customer has requested notification, notifying the customer that the authorization request has been**

received by transmitting a notification to a cell phone or a cellular network-connected communications device associated with the customer; and

Horie discloses this element. Horie discloses that “when [a] card 10 owned by a card user is used for payment transactions via card transaction terminal devices 1 to 3, card authentication processing is performed between card transaction terminal devices 1 to 3 and each authentication host via CAFIS 8, and an email is sent from the side of sever 4 to the mobile phone 11 owned by the card user and the PC 12 owned by the card user at home to notify the user that there was a card payment transaction.” Ex. 1006, [0044]; Ex. 1003 ¶ 140.

Horie further discloses an embodiment where “when a card payment transaction occurs, the user is automatically notified of the transaction via a wireless information terminal device such as a pre-specified mobile phone.” *Id.* at [0018]; Ex. 1003 ¶ 141. Horie goes on to disclose that such notification occurs “by sending and receiving specific data via a normal phone line of a mobile phone” Horie, [0020]; Ex. 1003 ¶ 141-142. The patent further discloses that “specific data indicating the content of card payment transactions can be transmitted from the mobile phone company host to the mobile phone 12, and the mobile phone 12 can display the context of the display by text, etc.” *Id.* at [0079]; At the time of the alleged invention, a POSITA would have understood that “text” sent to a mobile phone would have typically been in the form of an SMS message, which

was the most common format used at the time for the delivery of text-based transmissions of data to and from mobile phones. *See* Ex. 1003 ¶ 142; Ex. 1008, Abstract, 1:53-63.

Therefore, Horie discloses “transmitting a notification to a cell phone . . . associated with the customer” because it discloses that when a customer’s profile indicates that a notification is requested, the notification is sent “to the mobile phone 11 owned by the card user.” A phone “owned” by a card user is a phone that is associated with user. Ex. 1003 ¶ 143.

- vi. *Element [1e]* – processing the transaction for payment authorization and, if the purchase is authorized, notifying the merchant substantially contemporaneously with the step of transmitting the notification to the cell phone or the communications device associated with the customer.**

Horie discloses this limitation. Horie discloses that “[t]he various types of information that have been read are sent as data to each card authentication host 5-6 (or CAFIS 8), thereby issuing a card authentication processing request (step 204).” Ex. 1006, [0048]. “Thereafter, the response is waited until it is received from the side of each card authentication host (step 205 No, step 206), but when the response is received (step 205 YES), then the content of the response is determined (step 207).” *Id.* at [0049]. “If the received response indicates that authentication is not possible (step 208 NO), a predetermined error processing is

performed (step 210), but if authentication is successful (step 208 YES), processing is performed according to the response content, and (step 209) processing is completed.” *Id.* at [0050]. Ex. 1003 ¶ 145.

Horie states that “[t]he authentication process is then performed based on the received information (step 304)” and that the “card authentication process is actually executed via the CAFIS 8.” *Id.* at [0054]. Therefore, Horie discloses that the information gathered at the merchant’s terminal device is sent to CAFIS 8 (or a related authentication host), and that CAFIS / authentication host itself actually executes the card authentication and authorization. Ex. 1003 ¶¶ 146-147.

Horie further discloses that “when using card payment transactions, both normal card authentication processing and card usage status notification via email are performed simultaneously.” Ex. 1006, [0043]. A POSITA would understand that two notifications which “are performed simultaneously” are performed “substantially contemporaneously” because “simultaneous” and “contemporaneous” are synonyms for each other. *See* Ex. 1003 ¶¶ 147-148.

2. *Dependent claim 2* – The method according to claim 1, wherein **authorization request includes the account information and a monetary amount, and **the notification** to the communications device associated with the customer in an SMS message including the monetary amount.**

See claim 1 above. Horie renders this claim obvious. Horie discloses that “when the [card authorization] process is started, card information, transaction details information, and other necessary information are sequentially read on the

card transaction terminal device side (steps 201, 202, and 203).” Ex. 1006, [0046]. Further, Horie discloses that “the card information includes card number information. Transaction details information, when using a credit card, includes the transaction type (CAT: product purchase, etc., ATM: cash advance, deposit/withdrawal, etc.), transaction amount (CAT: purchase amount, etc., ATM: cash advance amount, etc.), transaction product classification (purchased product type, etc.), transaction product classification (purchased product type, etc.), payment method, etc. (lump sum, split, etc.), when using a debit card, transaction type (CAT: product purchase, etc., ATM: balance inquiry, deposit/withdrawal, etc.), transaction settlement Examples include the amount (CAT: purchase amount, etc., ATM: acquisition amount, etc.), transaction product classification, payment method, etc. Other necessary information includes ID information for each card transaction terminal, card password information input by the user, and the like.” *Id.* at [0047]; Ex. 1003 ¶ 151.

Horie further discloses an embodiment where “when a card payment transaction occurs, the user is automatically notified of the transaction via a wireless information terminal device such as a pre-specified mobile phone.” *Id.* at [0018]; Ex. 1003 ¶ 153. Horie goes on to disclose that such notification occurs “by sending and receiving specific data via a normal phone line of a mobile phone” Horie, [0020]. The patent further discloses that “specific data indicating the

content of card payment transactions can be transmitted from the mobile phone company host to the mobile phone 12, and the mobile phone 12 can display the context of the display by text, etc.” *Id.* at [0079]. At the time of the alleged invention, a POSITA would have understood that “text” sent to a mobile phone would have typically been in the form of an SMS message, which was the most common format used at the time for the delivery of text-based transmissions of data to and from mobile phones. *See* Ex. 1003 ¶¶ 153-154; Ex. 1008, Abstract, 1:53-63.

Finally, Horie discloses that the notification “sent to the user shows the type of card used for card payment transactions, card number, transaction date and time, card usage store name, card transaction terminal device ID, processing number, authorization number, purchased product category, transaction type (purchase, loan, etc.), and payment amount.” *Id.* at [0069]; Ex. 1003 ¶ 152.

B. GROUND 2: Claims 1-2 should be cancelled as obvious by Horie and the knowledge of a POSITA.

Horie and the knowledge of a POSITA discloses each element of claims 1 and 2 and therefore renders obvious each challenged claim 1 and 2 as obvious (“Ground 2”).

1. Independent claim 1.

i. Preamble – A payment authorization method, which comprises:

See analysis for claim 1, preamble, in Section VIII.A.1.i.

- ii. ***Element [1a]*** – gathering, at a merchant’s, account information for payment of a customer’s purchase;

See analysis for claim 1, element a, in Section VIII.A.1.ii.

- iii. ***Element [1b]*** – transmitting an authorization request from the merchant’s to a financial authorization system requesting payment authorization for the customer’s purchase

See analysis for claim 1, element b, in Section VIII.A.1.iii.

- iv. ***Element [1c]*** – checking whether or not a profile is present with regard to the customer and, if the profile is present, checking whether or not the customer has requested notification regarding the authorization request;

See analysis for claim 1, element c, in Section VIII.A.1.iv.

- v. ***Element [1d]*** – if the customer has requested notification, notifying the customer that the authorization request has been received by transmitting a notification to a cell phone or a cellular network-connected communications device associated with the customer; and

See analysis for claim 1, element d, in Section VIII.A.1.v.

- vi. ***Element [1e]*** – processing the transaction for payment authorization and, if the purchase is authorized, notifying the merchant substantially contemporaneously with the step of transmitting the notification to the cell phone or the communications device associated with the customer.

See analysis for claim 1, element e, in Section VIII.A.1.vi.

- 2. ***Dependent claim 2*** – The method according to claim 1, wherein **authorization request** includes the account information and a monetary amount, and **the notification** to the communications device associated with the customer in an SMS message including the monetary amount.

See analysis for claim 2 in Section VIII.A.2. To the extent that Horie does not disclose sending an SMS message to the customer, this would have been obvious in view of the disclosure of Horie. Ex. 1003 ¶ 155. Although Horie does not expressly use the term “SMS,” Horie discloses that “specific data indicating the content of card payment transactions can be transmitted from the mobile phone company host to the mobile phone 12, and the mobile phone 12 can display the content on the display by text, etc.” Horie, [0079]. At the time of the alleged invention, a POSITA would have understood that “text” sent to a mobile phone would have typically been in the form of an SMS message, which was the most common format used at the time for the delivery of short-form, text-based transmissions of data to and from mobile phones. *See* Ex. 1003 ¶ 156; Ex. 1008, Abstract, 1:53-63.

C. GROUND 3: Claims 3-5 should be cancelled as obvious by Horie in view of Kobayashi.

1. ***Dependent claim 3*** – The method according to claim 1, which further comprises **prompting the customer to return a response to the notification** and authorizing the purchase only when a proper response is returned.

See claim 1 above. Horie and Kobayashi render this claim obvious. Ex. 1003 ¶ 158. Horie discloses that “although[, in one embodiment,] an email is sent to notify the user after the card authentication process in the card payment transaction, **the e-mail can also be sent, for example, during the card authentication**

process. In such a case, for example, it would be possible to prevent fraudulent card use by making it possible to issue a transaction cancellation request to the authentication hosts 5 to 6 via the mobile phone 11.” Ex. 1006, [0073]. Thus, Horie discloses “prompting the customer to return a response to the notification and authorizing the purchase only when a proper response is returned” because in one embodiment, when the customer is notified of the transaction, he/she has the ability to “issue a transaction cancellation request” which means that if the customer does not authorize or approve the transaction, it can be cancelled. Ex. 1003 ¶ 159. Therefore, if the customer does issue such a request, the customer “return[s] a response to the notification” and the purchase will not be authorized because a proper response was not given. Conversely, this Horie disclosure also contemplates that if the customer does not “issue a transaction cancellation request” then the customer implicitly returns a response that the transaction is approved, and therefore the authorization will occur because a proper response was given. Ex. 1003 ¶ 159.

Kobayashi also renders this claim obvious. Kobayashi discloses that “[w]hen set to a mode in which identity verification is performed by a mobile phone, the phone number of the mobile phone registered corresponding to the card number is searched and obtained from database 12 (step S6), and the phone number of the mobile phone is automatically dialed (step S7).” Ex. 1007, [0057]; Ex. 1003 ¶ 160.

Then “[i]f the user presses the call button (off-hook) in response to the ringing, etc., of the mobile phone 6 (step S8), the center 1 receives this response (“response received” in step S9) and sends guidance (step S10). The guidance may be audio or text information.” *Id.* at [0058]. Next, “[t]he user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step S11). The input information indicating whether the card can be sued or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.” *Id.* at [0060]. Finally, “[t]he center 1 judges the card usage permission information transmitted from the mobile phone 6, determines whether the card can be used (step S12), and notifies the member store terminal 2 of the determination result of the usage permission.” *Id.* at [0061]; Ex. 1003 ¶¶ 160-161.

Finally, Kobayashi discloses that when the password entered by the user does not match the password on file, even after multiple retries “it is determined that the card cannot be used. Based on the determination result of the password authentication unit 19, the card usage permission notification unit 17 notifies the member store terminal 2 whether the card can be used or not.” Ex. 1007, [0070]; Ex. 1003 ¶ 162. However, if the passwords match, “it is determined that the user’s identity has been verified and that the card can be used.” Kobayashi, [0069]. Thus, Kobayashi discloses that the card transaction will only be authorized if it receives a

proper response. Ex. 1003 ¶ 162.

2. *Dependent claim 4* – The method according to claim 3, wherein the **response includes a personal identifier associated with the customer.**

See claim 3 above. Horie and Kobayashi render this claim obvious. Ex. 1003 ¶ 164. Horie discloses that “although[, in one embodiment,] an email is sent to notify the user after the card authentication process in the card payment transaction, the e-mail can also be sent, for example, during the card authentication process. In such a case, for example, **it would be possible to prevent fraudulent card use by making it possible to issue a transaction cancellation request to the authentication hosts 5 to 6 via the mobile phone 11.**” Ex. 1006, [0073]; Ex. 1003 ¶ 165.

Kobayashi discloses “an example of the configuration of the database 12 that manages card members in an embodiment of the present invention. Referring to Fig. 3, in addition to the card number (identification information) and personal information such as the card member’s name, gender, age, and address, each entry includes information on whether or not to use a mobile phone to verify the identity of the member when using the card, the phone number of the member’s mobile phone if the member’s identity is verified using the mobile phone, and password information.” Ex. 1007, [0052]; Ex. 1003 ¶ 166.

Finally, Kobayashi discloses “[t]he user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step

S11). The input information indicating whether the card can be used or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.” Kobayashi, [0060]; Ex. 1003

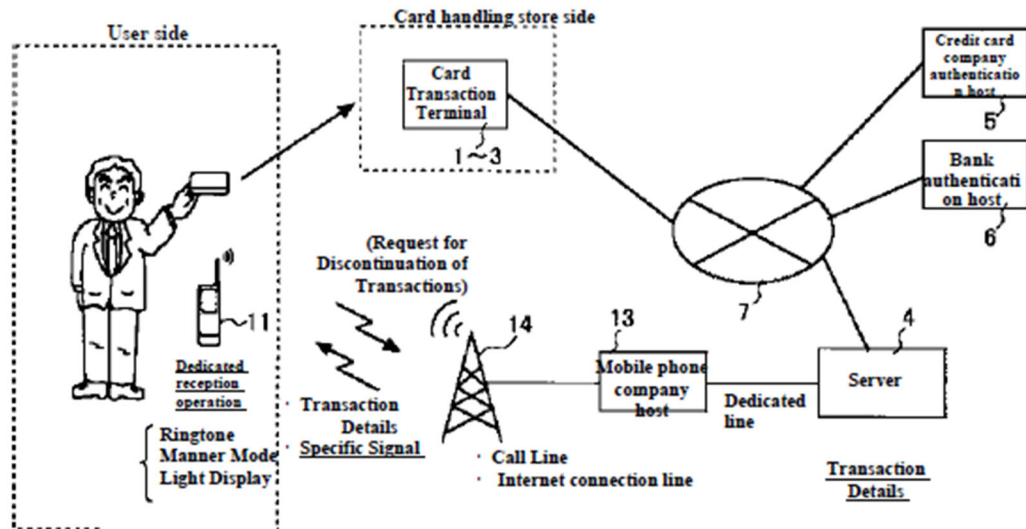
¶ 167. Therefore, Kobayashi discloses a response that includes a personal identifier because the user inputs a “number and #” that is “agreed with the card company.” This language contemplates that at the time of the card creation, the user provides the card company with an agreed upon number, whether it be the card number itself or a PIN number. The card company would keep this number on file and when the customer provides it during the authentication process, the card company would use it to verify the identity of the customer, making “number and #” a personal identifier. Ex. 1003 ¶ 167.

3. Independent claim 5.

i. Preamble – A charge card processing method, which comprises:

To the extent the preamble is limiting, it is disclosed by Horie. Horie “relates to a card usage status notification method that automatically notifies a card user, etc. that a card payment transaction has occurred via a network, and a card payment transaction system using the same method.” Ex. 1006, at [0001]; Ex. 1003 ¶ 169.

The method of Horie is shown in Figure 9, below:



Ex. 1006, Fig. 9.

ii. **Element [5a]** – inputting a **transaction request** to a **stationary merchant terminal** disposed at a **merchant location**;

Horie renders this limitation obvious. Ex. 1003 ¶ 171. Horie discloses that “when [a] card 10 owned by a card user is used for **payment transactions** via **card transaction terminal devices 1 to 3**, **card authentication processing** is performed between **card transaction terminal devices 1 to 3** and each authentication host via CAFIS 8, and an email is sent from the side of sever 4 to the mobile phone 11 owned by the card user and the PC 12 owned by the card user at home to notify the user that there was a card payment transaction.” Ex. 1006, [0044].

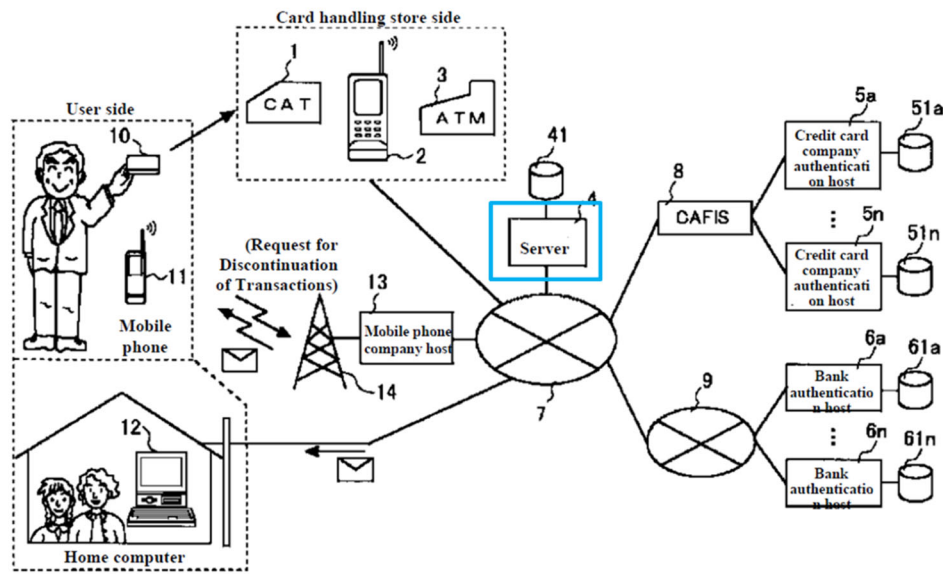
Horie further discloses a “**card payment transaction system** according to the first embodiment of the present invention includes a **CAT 1 installed in a card handling store**” and “**an ATM 3 installed in a bank.**” Horie, [0039]. A POSITA would have understood that because these devices would be “installed” in a store

or bank they would be connected to the network by a wired (*i.e.* landline) connection. Ex. 1003 ¶¶ 172-173. This understanding is further supported by Horie’s distinction between a “CAT” and a “wireless CAT,” which shows that the “CAT 1” would have had a wired landline. *See* Ex. 1006, [0039]; Ex. 1003 ¶ 172.

- iii. *Element [5b]* – processing the transaction request with the merchant terminal, including a transmission of a first authorization request to a remote processing facility and receipt of a notification that authorization has been accepted or declined;**

Horie discloses this element. Horie discloses “a card payment transaction system . . . [that] includes a CAT 1 installed in a card handling store, a portable wireless CAT 2 suitable for use in door-to-door sales, etc., and an ATM 3 installed in a bank etc., an information processing company server (hereinafter simply referred to as server) 4 that executes various processes for notifying card usage status” and “credit card authentication host[s] 5a to 5n that perform[] card authentication processing when using a credit card, bank authorization hosts 6a to 6n for performing card authentication processing when using a debit card (cash card), and a network 7 that connects them.” Ex. 1006, [0039]; Ex. 1003 ¶ 175. The server is highlighted in Figure 1 below.

[FIG. 1]



Ex. 1006, Fig. 1 (annotated).

Additionally, Horie also discloses “a credit card authentication host 5a to 5n that performs card authentication processing when using a credit card, bank authentication hosts 6a to 6n for performing card authentication processing when using a debit card (cash card), and a network 7 that connects them.” Ex. 1006, [0039]. These are further examples of Horie’s disclosure of transmission of a first authorization request to a remote processing facility.

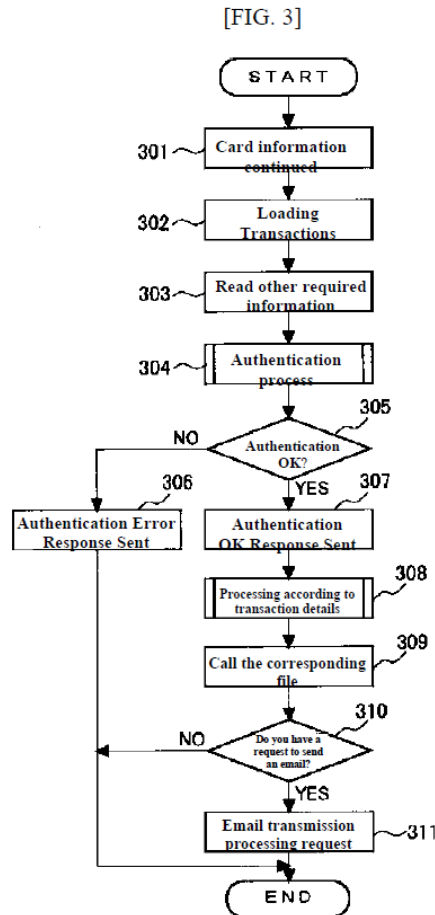
As can be seen in Fig. 1, the server 4 and authentication hosts 5a-n and 6a-n are “remote” compared to the card transaction terminals because the servers/hosts are located in different sites than the card transaction terminals. Therefore, Horie discloses transmission of the first authorization request to a remote processing facility. Ex. 1003 ¶ 176.

Further, “Fig. 3 shows the processing on the card authentication host side when using a card payment transaction.” *Id.* at [0052]. “As shown in Fig. 3, based on the authentication processing request from the side of the card transaction terminal device, card information, transaction content information, and other necessary information transmitted from the side of the card transaction terminal device are sequentially received and loaded on the side of the card authentication host (steps 301, 302, and 303).” *Id.* at [0053]. Then “[t]he authentication process is then performed based on the received information (step 304).” *Id.* at [0054]. “If the authentication is not successful (step 305 NO), a signal indicating an authentication error is sent to the card transaction terminal devices 1 to 3 as a response to the authentication request (step 306), and the process ends. On the other hand, when authentication is successful (step 305 YES), a signal indicating authentication OK or data, etc., required for processing on the side of the card transaction terminal device is transmitted to the side of the card transaction terminal device 1-3 (step 307), and various processing is then performed according to the transaction content (step 308).” *Id.* at [0055]-[0056]; Ex. 1003 ¶ 177.

Therefore, Horie discloses a “receipt of a notification that authorization has been accepted or declined” because Horie discusses a “signal” that is sent to the card transaction terminal device, and the signal can either indicate “an authentication error” or “authentication OK” either of which would provide a

notification to the merchant that the authorization has been accepted or declined.

Ex. 1003 ¶ 178.



Flowchart showing card authentication host side processing

Ex. 1006, Ex. 3.

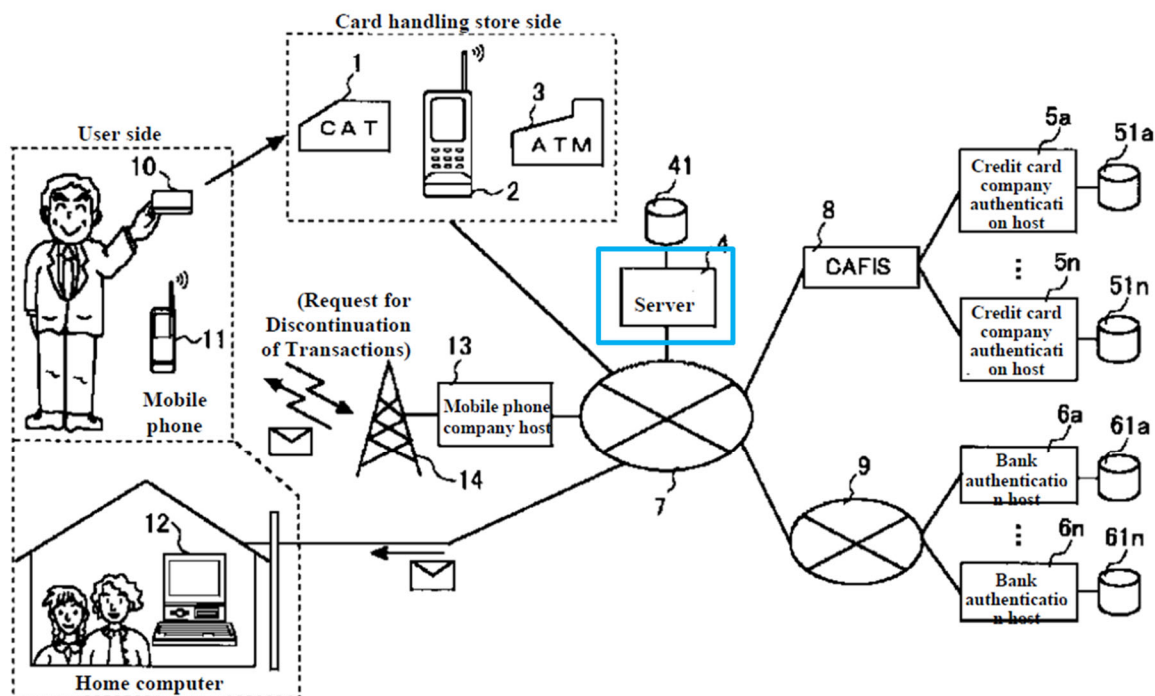
- iv. **Element [5c] – transmitting a second authorization request from a remote processing facility to a mobile communication device of a customer associated with the requested transaction through a cellular network; and**

Horie and Kobayashi render this element obvious. Ex. 1003 ¶ 179. Horie discloses a method where “a predetermined file is called for determining whether

or not to notify the user of the card payment transaction via email (step 309).” Ex. 1006, [0057]. “This file is a file stored in each of the recording devices 51 to 61 of the card authentication hosts 5 to 6 . . . [and] the corresponding electronic data is stored for each card number. Whether or not notification is to be provided by email is recorded in advance.” *Id.* Further, Horie discloses, that “although[, in one embodiment,] an email is sent to notify the user after the card authentication process in the card payment transaction, the e-mail can also be sent, for example, during the card authentication process. In such a case, for example, it would be possible to prevent fraudulent card use by making it possible to issue a transaction cancellation request to the authentication hosts 5 to 6 via the mobile phone 11.”

Ex. 1006, [0073]. Therefore, Horie discloses “transmitting a second authorization request” because in one embodiment of the method, the customer can “issue a transaction cancellation request” in response to the authentication host which is requesting authorization. Ex. 1003 ¶ 180. Further, as can be seen in figure 1 below, the request is sent from the server to the cell phone via a cellular network.

[FIG. 1]



Ex. 1006, Fig. 1 (annotated).

Kobayashi discloses “an example of the configuration of the database 12 that manages card members in an embodiment of the present invention. Referring to Fig. 3, in addition to the card number (identification information) and personal information such as the card member’s name, gender, age, and address, each entry includes information on whether or not to use a mobile phone to verify the identity of the member when using the card, the phone number of the member’s mobile phone if the member’s identity is verified using the mobile phone, and password information.” Ex. 1007, [0052]; Ex. 1003 ¶ 181.

Finally, Kobayashi discloses “[t]he user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step S11). The input information indicating whether the card can be used or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.” *Id.* at [0060]. Therefore, Kobayashi discloses “transmitting a second authorization request” because the card company calls the customer for authorization and in response the customer enters information as to “whether the card can be used or not.” Ex. 1003 ¶ 182.

- v. ***Element [5d]* – authorizing the requested transaction only if authorization has been accepted for the first authorization request and a proper response has been received by the remote processing facility to the second authorization request.**

Horie and Kobayashi render this element obvious. Ex. 1003 ¶ 183. Horie discloses “when card 10 owned by a card user is used for payment transactions via card transaction terminal devices 1 to 3, card authentication processing is performed between card transaction terminal devices 1 to 3 and each authentication host via CAFIS 8, and an e-mail is sent from the side of server 4 to the mobile phone 11 owned by the card user and the PC 12 owned by the card user at home to notify the user that there was a card payment transaction.” Ex. 1006, [0044]. Horie further discloses that “although[, in one embodiment,] an email is sent to notify the user after the card authentication process in the card payment transaction, the e-mail can also be sent, for example, during the card authentication

process. In such a case, for example, it would be possible to prevent fraudulent card use by making it possible to issue a transaction cancellation request to the authentication hosts 5 to 6 via the mobile phone 11.” Ex. 1006, [0073]; Ex. 1003 ¶¶ 184-185.

Kobayashi also renders this claim obvious. Ex. 1003 ¶ 186. Kobayashi discloses that “[w]hen set to a mode in which identity verification is performed by a mobile phone, the phone number of the mobile phone registered corresponding to the card number is searched and obtained from database 12 (step S6), and the phone number of the mobile phone is automatically dialed (step S7).” Ex. 100_, [0057]. Then “[i]f the user presses the call button (off-hook) in response to the ringing, etc., of the mobile phone 6 (step S8), the center 1 receives this response (“response received” in step S9) and sends guidance (step S10). The guidance may be audio or text information.” *Id.* at [0058]. Next, “[t]he user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step S11). The input information indicating whether the card can be used or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.” *Id.* at [0060]. Finally, “[t]he center 1 judges the card usage permission information transmitted from the mobile phone 6, determines whether the card can be used

(step S12), and notifies the member store terminal 2 of the determination result of the usage permission.” *Id.* at [0061]; Ex. 1003 ¶ 186.

Therefore, Horie renders the first part of this claim obvious because it discloses a “first authorization request” because in the process the card transaction terminals located in the merchant stores communicate with the authentication hosts, asking for authorization for the purchase. Ex. 1003 ¶ 185. Kobayashi renders the second part of the claim obvious because it discloses a “second authorization request” and a “proper response” because in the method of Kobayashi, the card center calls the card holder and provides “guidance” on the transaction. Ex. 1003 ¶ 186. In response, the customer inputs information “indicating whether the card can be used or not.” In response to the response from the customer, the center “notifies the member store terminal” whether or not authorization is provided based on whether a proper response is received from the customer. Ex. 1003 ¶ 186.

D. GROUND 4: Claims 6-7 should be cancelled as anticipated by Kano.

1. Independent claim 6.

i. Preamble – A charge card processing method, which comprises:

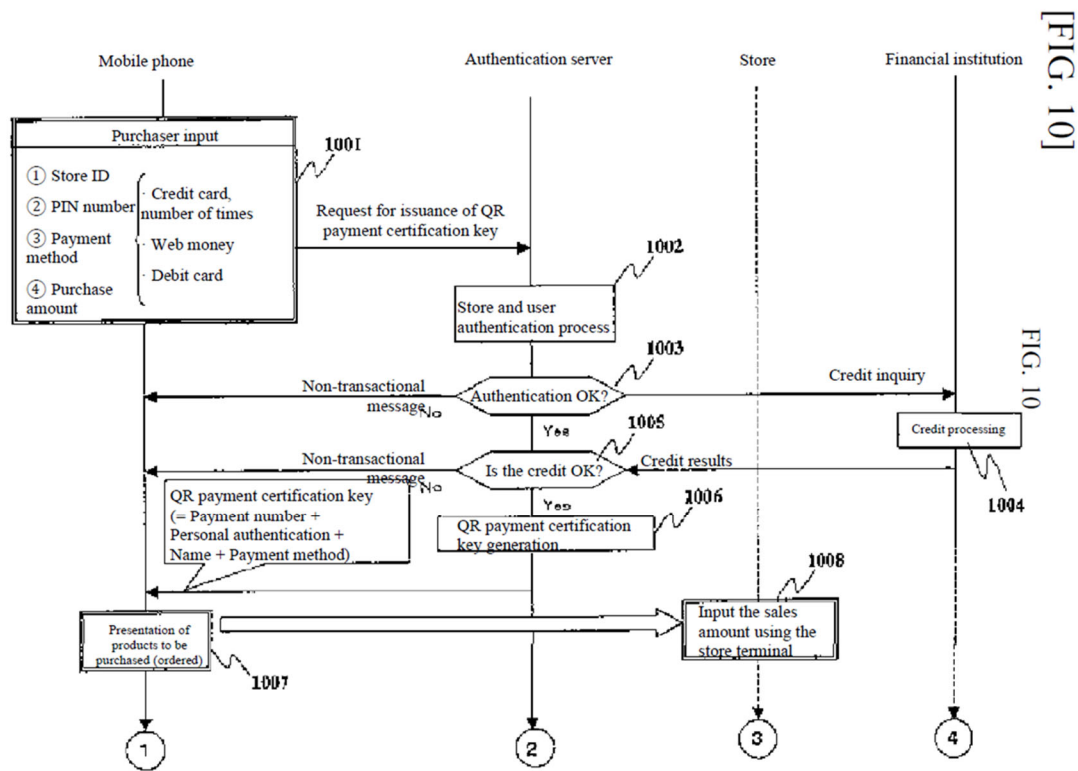
To the extent the preamble is limiting, it is disclosed by Kano. Ex. 1003 ¶ 187. Kano discloses “[t]he present invention relates to a commercial transaction method, a commercial transaction device and a commercial transaction system that

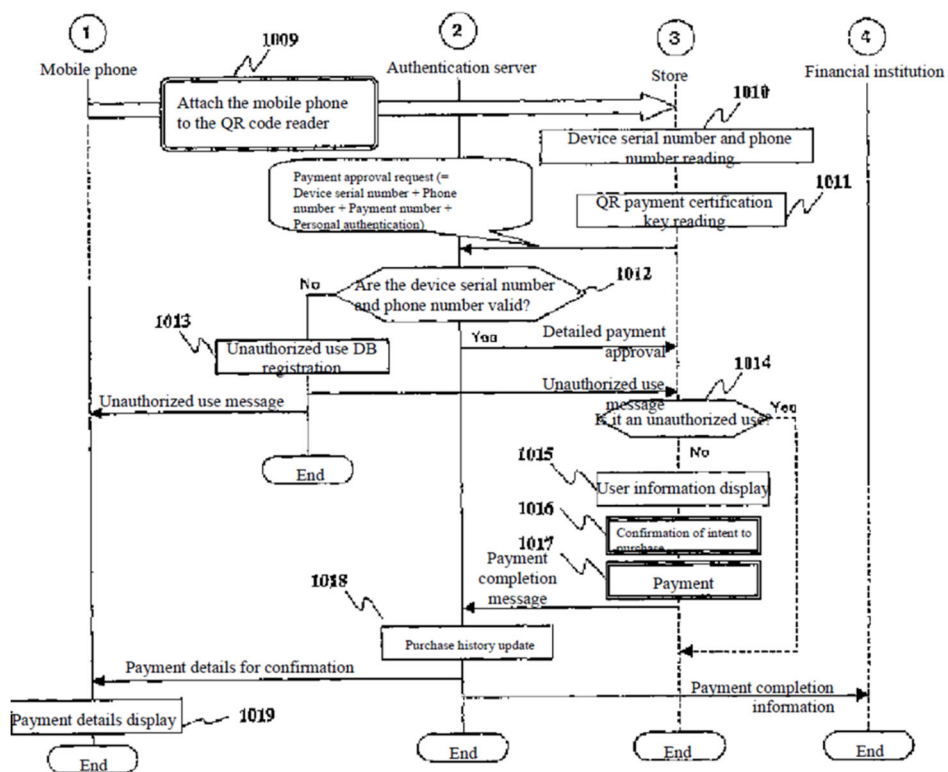
can be sued for payment of products purchased at various stores such as supermarkets, electronic stores, opened on Internet servers, or vending machines such as for potable drinking water, using terminals that can be connected to a network such as via mobile phones.” Ex. 1011, 6:51-7:3; Ex. 1003 ¶¶ 188-189.

ii. Element [6a] – preauthorizing an imminent given transaction by transmitting a preauthorization for the imminent given transaction from a customer to a financial authorization system;

Kano discloses this limitation. Ex. 1003 ¶ 190. Kano discloses “flowcharts illustrating how decisions are made when purchasing products using a mobile phone 1 at general stores such as supermarkets.” Ex. 1011, 13:31-32. In the disclosed method “the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID as the identification information of the store from which he or she intends to purchase the product. The user then inputs his or her personal ID number . . . , the payment method, and the purchase price of the product (step 1001).” *Id.* at 13:33-37. The payment method can be a “credit card payment[], web money payment[], [or] debit card payment[], and if the credit card payment is selected, the number of payments and the credit card number are inputted.” *Id.* at 13:39-41; Ex. 1003 ¶ 191. When the user completes the input “the transmission operation is performed. Then the information input in step 1001 is sent to the authentication server 41 as the QR authorized certification key issuance request.” *Id.* at 13:46-47.

See Figs. 10 and 11 below.





[FIG. 11]

FIG. 11

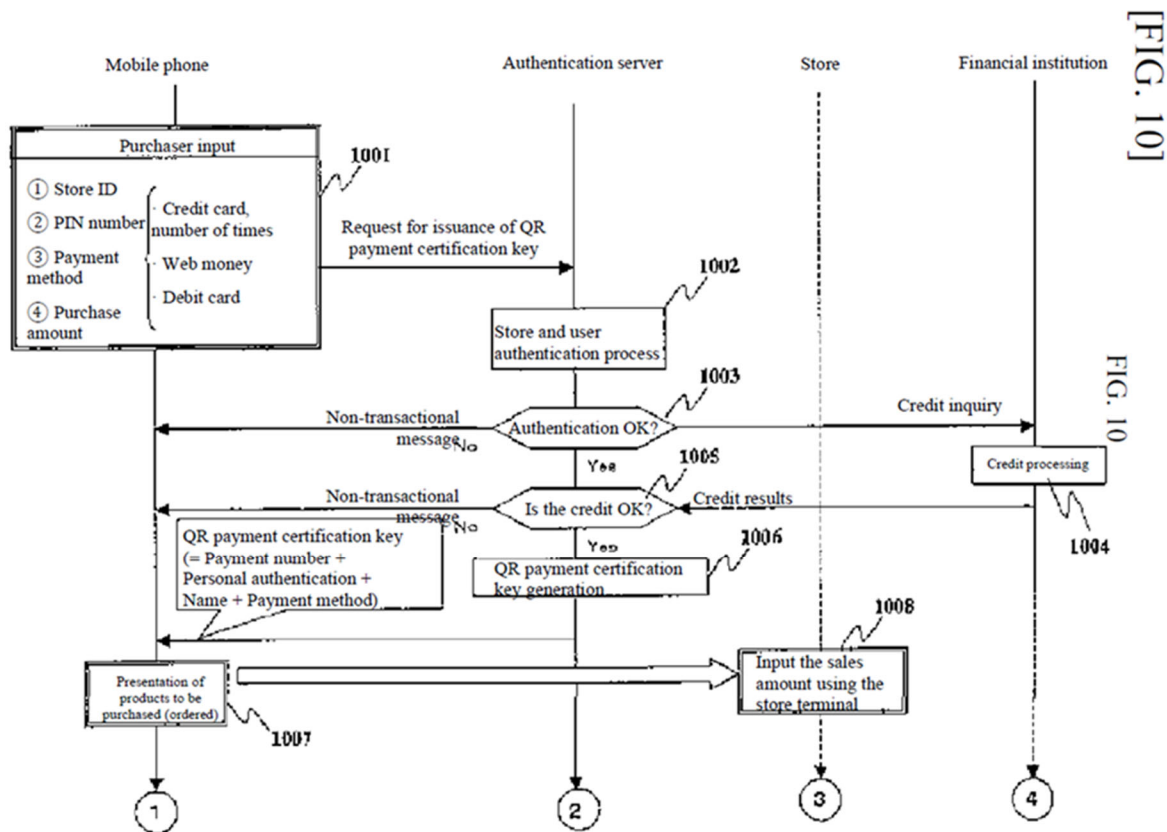
Ex. 1011, Figs. 10 and 11.

The method of Kano discloses “preauthorization” because when the user inputs such things as the store where the purchase will occur, the payment method, and the purchase price, the user is providing the card center with authorization to approve a purchase of specific items before the transaction with the store has occurred or even started, the very essence of preauthorization. Ex. 1003 ¶ 192.

- iii. *Element [6b]* – subsequently inputting a **transaction request** concerning the given transaction at a **merchant terminal** disposed at a **merchant location**;

Kano discloses this limitation. Ex. 1003 ¶ 193. Kano discloses that when the transaction is authorized, “a QR authorized certification key consisting of a

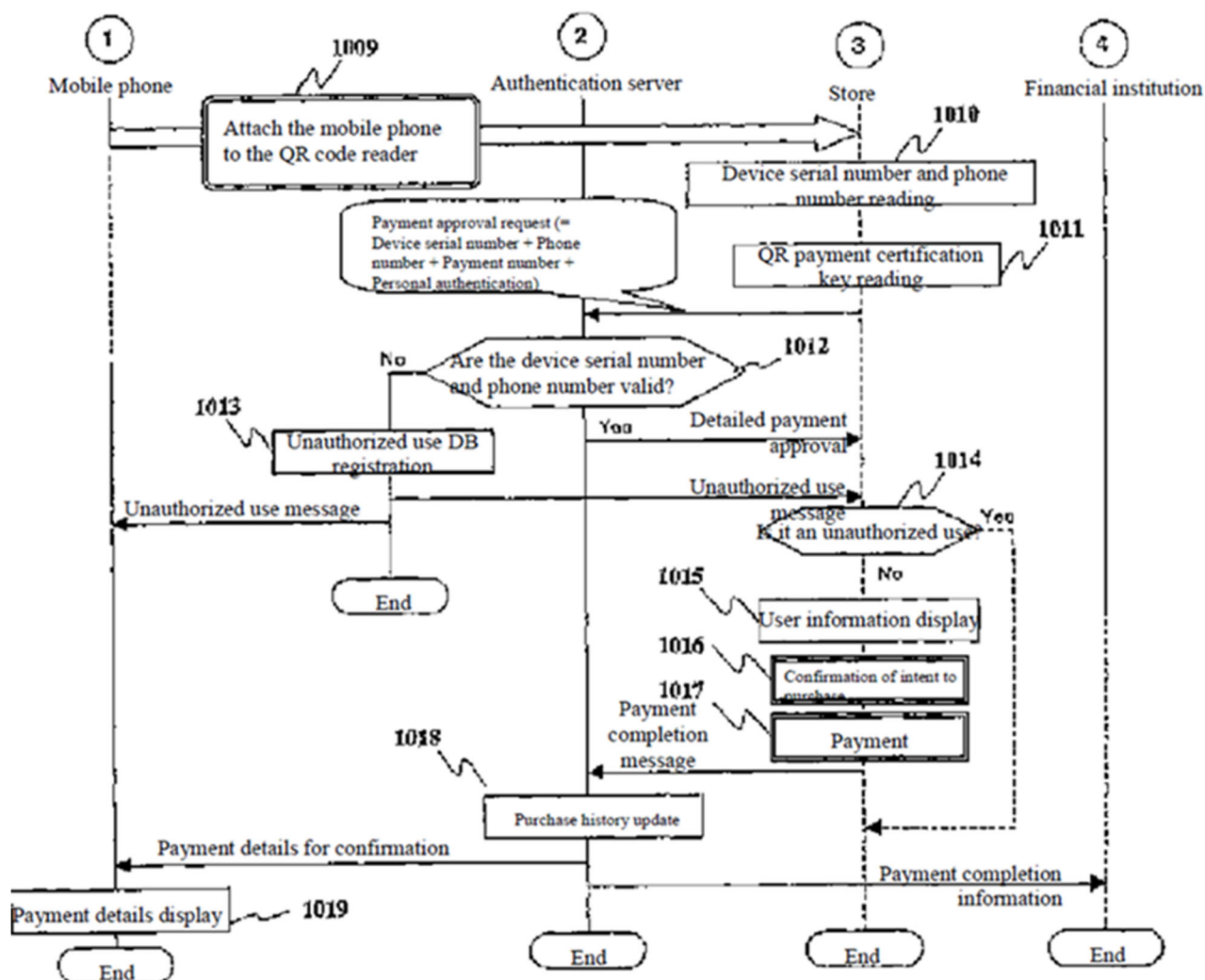
two-dimensional code as shown in Fig. 3(d) is generated (step 1006) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and a method of authorization.” Ex. 1011, 14:12-15. Then “the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 1007). The store staff enters the price of the desired purchase item using the store terminal (step 1008).” *Id.* at 14:20-22; Ex. 1003 ¶ 194.



Ex. 1011, Fig. 10.

- iv. *Element [6c]* – processing the transaction request at the **merchant terminal**, including a transmission of **an authorization request** for the given transaction to the financial authorization system;

Kano discloses the limitation. Ex. 1003 ¶ 195. Kano discloses that “the user inserts and attaches the mobile phone 1 with the QR authorized key 1201 displayed to the **reader portion of the QR code reader 21 attached to the store terminal 22** (step 1009). “The QR code reader 21 then reads the QR authorized certification key 1201 displayed on the display 11 of the mobile phone 1 (step 1011), and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1010), and forwards the information to the store terminal 22.” Ex. 1011, 14:23-27. “The store terminal 22 then sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from the mobile phone 1 to **the authentication server 41 as a payment approval request.**” *Id.* at 14:28-30; Ex. 1003 ¶ 196.



Ex. 1011, Fig. 11.

Thus, Kano discloses “processing the transaction request at the merchant terminal” because after the store scans the items desired to be purchased, the customer inserts the QR code into a QR reader. Ex. 1003 ¶ 196. The QR code serves as a transaction request because it provides the store terminal with information about a payment method and the specific items are included in the QR authorization code. Kano also discloses “an authorization request” because in the

method the store terminal sends all the information gathered from the QR code scan to an authentication server “as a payment approval request.” Ex. 1003 ¶ 197.

- v. *Element [6d]* – transmitting a response to the **authorization request** from the financial authorization system to the **merchant terminal**, and thereby authorizing the transaction request at the merchant’s if the **preauthorization** from the customer is available in the financial authorization system, and otherwise contacting the customer for authorization or declining the authorization request.

Kano discloses this limitation. Ex. 1003 ¶ 198. Kano discloses that “[w]hen the authentication server 41 receives a **request for approval**, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1012). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (Fig. 9) (step 1013), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.” Ex. 1011, 14:35-40. Then “[i]n **the store terminal 22**, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1014).” *Id.* at 14:44-45; Ex. 1003 ¶ 199.

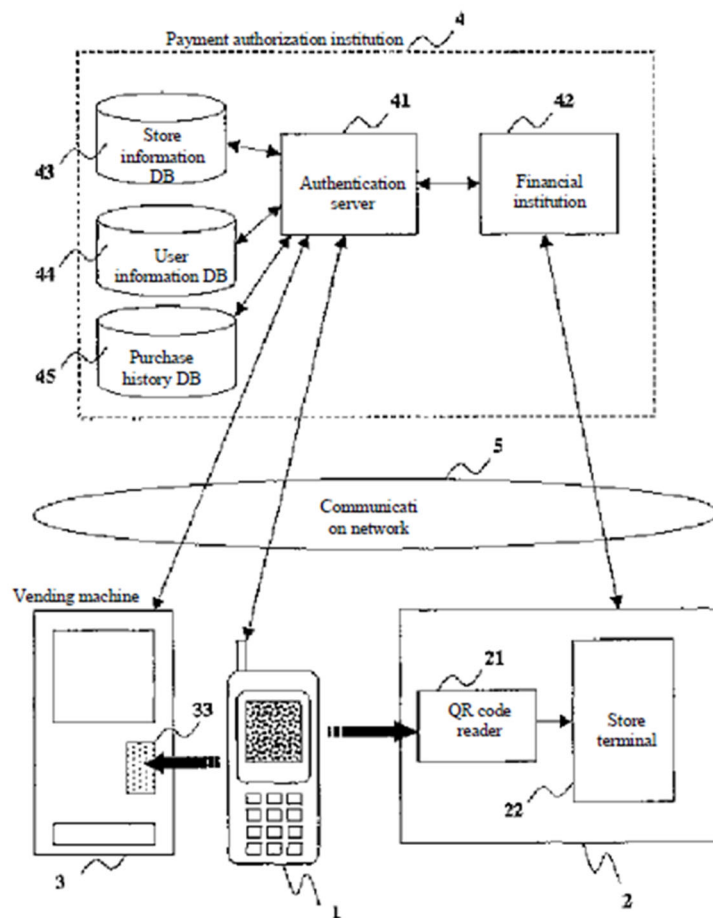
Kano discloses that, on the other hand, “in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the **QR authorized certification key 1201** received from the **store terminal 22** is recognized as a genuine one issued by the store terminal

22, the authentication server 41 returns the detailed settlement approval to the store terminal 22.” *Id.* at 14:47-50. “The store terminal 22 displays all or part of the received detailed authorization information on the display unit as user information (step 1015).” *Id.* at 14:54-55. Then “[t]he store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and the price of the products they wish to purchase (step 1016). If there is a response confirming the purchase intention from the person, the transaction is completed by operating the transaction button (step 1017).” *Id.* at 14:55-59; Ex. 1003 ¶ 200.

Kano further discloses that “[t]he store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1614). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1615).” *Id.* at 18:44-47.

[FIG. 1]

FIG. 1



Ex. 1011, Fig. 1.

Kano therefore discloses “transmitting a response to the authorization request” because the authentication server will either return an “unauthorized use message” or a “detailed settlement approval.” Ex. 1003 ¶ 199. Kano also discloses authorizing if the preauthorization is available in the financial system because, in Kano, the authentication server returns a “detailed settlement approval” if the “information (all or part) on the QR authorized certification key 1201

received from the store terminal 22 is recognized as a genuine one.” The QR code, if genuine, is one that is generated as a result of the customer providing preauthorization for the products he or she wishes to purchase. *See* discussion of QR code generation in VIII.D.1.ii, *supra*. Finally, Kano discloses “otherwise contacting the customer” because when authorization is provided, the in-store terminal displays the approval message. Ex. 1003 ¶ 200.

2. *Dependent claim 7* – The method according to claim 6, wherein the **preauthorization from the customer includes a maximum amount to be authorized for the transaction and a time period within which the preauthorization is valid.**

Kano anticipates this claim. Ex. 1003 ¶ 202. Kano discloses that “the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID as the identification information of the store from which he or she intends to purchase the product. The user then inputs his or her personal ID number . . . , the payment method, and the purchase price of the product (step 1001).” Ex. 1011, 3:33-37; Ex. 1003 ¶ 203. Further, Kano discloses that when the transaction is authorized, “a QR authorized certification key consisting of a two-dimensional code as shown in Fig. 3(d) is generated (step 1006) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and a method of authorization.” Ex. 1011, 14:12-15. Kano further discloses that “since the QR authorized certification key

1301 is only valid once, it is automatically deleted after a predetermined period of time. In addition, the financial institution 42 that receives the approval completion information performs procedures to withdraw the amount from the user's designated account.” *Id.* at 15:7-8; Ex. 1003 ¶¶ 203-204.

E. GROUND 5: Claims 6-7 should be cancelled as obvious by Kano and the knowledge of a POSITA.

1. Independent claim 6.

i. Preamble – A charge card processing method, which comprises:

See analysis for claim 6, preamble, in Section VIII.D.1.i.

ii. Element [6a] – preauthorizing an imminent given transaction by transmitting a preauthorization for the imminent given transaction from a customer to a financial authorization system;

See analysis for claim 6, element a, in Section VIII.D.1.ii.

iii. Element [6b] – subsequently inputting a transaction request concerning the given transaction at a merchant terminal disposed at a merchant location;

See analysis for claim 6, element b, in Section VIII.D.1.iii.

iv. Element [6c] – processing the transaction request at the merchant terminal, including a transmission of an authorization request for the given transaction to the financial authorization system;

See analysis for claim 6, element c, in Section VIII.D.1.iv.

- v. *Element [6d]* – transmitting a response to the **authorization request** from the financial authorization system to the **merchant terminal**, and thereby authorizing the transaction request at the merchant's if the **preauthorization** from the customer is available in the financial authorization system, and otherwise contacting the customer for authorization or declining the authorization request.

See analysis for claim 6, element d, in Section VIII.D.1.v.

- 2. *Dependent claim 7* – The method according to claim 6, wherein the **preauthorization** from the customer includes a maximum amount to be authorized for the transaction and a time period within which the preauthorization is valid.

See analysis for claim 7 in Section VIII.D.2. To the extent that Kano does not disclose a maximum amount to be authorized, this would have been obvious in view of the disclosure of Kano and the knowledge of a POSITA. Ex. 1003 ¶ 205. Part of the initial inputs from the user include “the payment method” and “the purchase price of the product.” Ex. 1011, 13:37; Ex. 1003 ¶ 206. When the transaction is authorized, Kano discloses that “a QR authorized certification key consisting of a two-dimensional code . . . is generated . . . and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and a method of authorization.” *Id.* at 14:12-15. Therefore, the QR code will include “a maximum amount to be authorized” because it will only allow for approval of the “purchase price of the product” that was inputted by the user. Ex. 1003 ¶ 206.

IX. Denial Under § 325(d) is Inappropriate.

The Board should not exercise its discretion under 35 U.S.C. § 325(d) to deny this Petition. None of the prior art in Ground 1 was of record or cited during examination of the '706 Patent. Thus, the first part of the *Advanced Bionics* framework is not met. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential) ("*Advanced Bionics*"). The Board should therefore institute review.

X. Discretionary Denial is Inappropriate.

The Board should not exercise its discretion under § 314(a) because there is no co-pending litigation between Petitioner Askeladden and the Patent Owner Calabrese Stemer, which means that the *Fintiv* framework does not apply. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020). The Board should thus decline to exercise its discretion under § 314(a) and institute *inter partes* review.

XI. Conclusion.

Petitioner respectfully requests that the Board institute review and find all challenged claims unpatentable.

Dated: January 2, 2024

Respectfully submitted,

By: /Alton L. Absher III/

Alton L. Absher III

Lead Counsel for Petitioner

CERTIFICATE OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. § 42.24(d) that the foregoing **Petition for *Inter Partes* Review** excluding any mandatory notices, table of contents, table of authorities, certificates of service or word count, or appendix of exhibits or claim listing, contains fewer than 14,000 words according to the word-processing program used to prepare this paper (Microsoft Word).

Dated: January 2, 2024

/Alton L. Absher III/
Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing Petition for *Inter Partes* Review was served on January 2, 2024 by Priority Mail Express upon the following counsel of record:

Lerner Greenberg Stemer LLP
PO Box 2480
Hollywood, FL 33022-2480

Dated: January 2, 2024

/Alton L. Absher III/
Counsel for Petitioner