

Inter Partes Review

U.S. Patent No. 10,713,656

Apple Inc. v. Carbyne Biometrics, LLC., Case IPR2024-00330

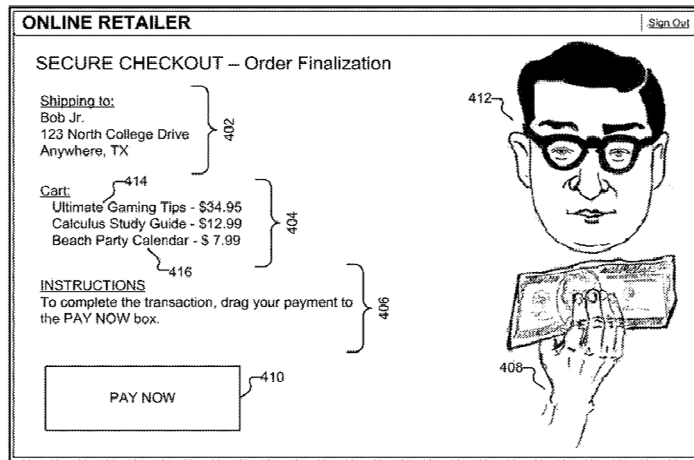
David O'Brien, Haynes and Boone, LLP
Hong Shi, Haynes and Boone, LLP
Kelly Lyle, Haynes and Boone, LLP
Representing Petitioner Apple

Claim 1 of '656 Patent

The inventive concept of the '656 Patent is capturing contextual information for subsequent to receiving the indication of the action taken by the user, which distinguishes prior art describing capturing contextual information for login.

- [1.0] A system, comprising:
- [1.1] a processor configured to:
- [1.2] receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;
- [1.3] render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
- [1.4] render, in the one or more interfaces, a transaction icon associated with the electronic transaction;
- [1.5] receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;
- [1.6] **subsequent to receiving the indication of the action taken by the user**, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;
- [1.7.1] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
- [1.7.2] performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
- [1.7.3] determining, based at least in part on the captured biometric information, that the user is alive; and
- [1.8] based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and
- [1.9] a memory coupled to the processor and configured to provide the processor with instructions.

'656 Patent



400 → FIG. 4

Increasing Feelings of Guilt

One reason that an otherwise honest person might engage in a fraudulent transaction is that the monetary value of the transaction is abstract. The more concrete the value of a transaction is, the more guilty a fraudster might feel when perpetrating the fraud. A \$20 bill, when held in a person's hand and presented to a merchant, is a tangible item with a concrete value. When the same amount of money is involved in an electronic transaction (e.g., the purchase of a book or set of magazines), the amount of money involved may seem less concrete.

('656 Patent) APPL-1001, 4:64-5:7; Reply, 5.

In some embodiments, an analysis of the photograph is performed as part of the transaction. Techniques for confirming that the object being photographed is alive (e.g., by taking multiple photographs in rapid succession) can be employed to help make sure that the fraudster isn't using camera 112 to photograph a printed picture of the legitimate user. The application of various rules, such as requiring that

('656 Patent) APPL-1001, 8:60-66; Pet. 3.

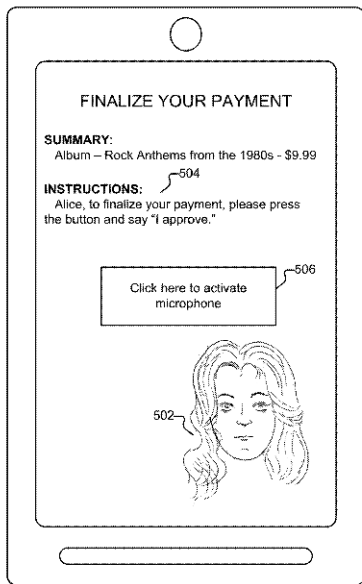


FIG. 6

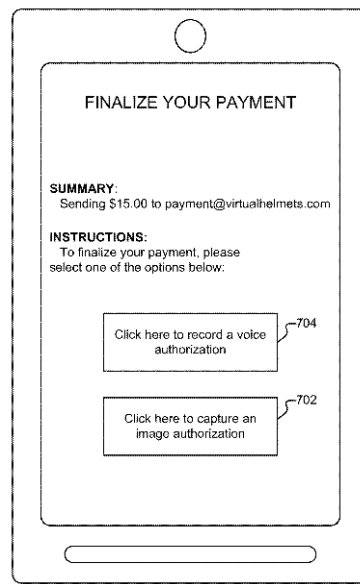


FIG. 7

('656 Patent) APPL-1001, FIGS. 4, 6, 7; Pet. 3; POR, 4-5.

Petitioner's Instituted Grounds

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 4–10, and 13–19	103(a) ¹	Stone, ² Hoyos, ³ Varghese ⁴
1, 4–10, and 13–19	103(a)	Stone, FFIEC Guidance ⁵
2, 3, 11, and 12	103(a)	Stone, Hoyos, Varghese, Borovsky ⁶
2, 3, 11, and 12	103(a)	Stone, FFIEC Guidance, Borovsky

Inst. Dec. 7.

Issues:

- Motivations to combine of Grounds
- Grounds 1 and 2: Limitations [1.2], [1.9]; limitations of claims 5, 8, 14, and 17.

Undisputed:

- Ground 1: Limitations [1.0]-[1.1], [1.3]-[1.8], including [1.6] resulted in allowance; limitations of claims 4, 6-7, 9, 13, 15-16, 18-19
- Grounds 3 and 4: Limitations of claims 2-3, 11-12.

Summary of Combinations

Combinations	'010	'656	'886
Stone and Hoyos	Ground 1		
Stone, Hoyos, and Varghese	Ground 2	Ground 1	Ground 1
Stone and FFIEC Guidance	Ground 3	Ground 2	Ground 2
Stone, Hoyos, Varghese, Borovsky		Ground 3	
Stone, Guidance, Borovsky		Ground 4	
Stone, Hoyos, Varghese, and Campbell			Ground 3
Stone, Guidance, and Campbell			Ground 4

Summary of Claim Landscape

General Claim Terms of Claim 1		'010	'656	'886
one or more processors		✓		✓
a processor			✓	
receive and store biometric info [for later comparison], wherein the biometric info is associated with an account			[1.2] ✓	
receive and associate a virtual likeness of a face		[1.2] ✓		
render [the/a] virtual likeness of a face of the account holder	a face of a recipient	[1.3]- ✓	✓	✓
		[1.5]		
The virtual likeness was selected as part of an enrollment				[1.2.2] ✓
capture contextual info	biometric info	✓	✓	✓
	subsequent to an interaction by a user, capture location data		✓	[1.3.1] ✓
fraud detection analysis	determine that the user is alive	✓	✓	✓
	comparison based on stored and captured biometric info		✓	
a memory coupled to and provide the [one or more processors/processor] with instructions.		[1.9] ✓	[1.9] ✓	✓

Claim 1 of '656 Patent

- [1.0] A system, comprising:
 - [1.1] a processor configured to:
 - [1.2] receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;
 - [1.3] render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
 - [1.4] render, in the one or more interfaces, a transaction icon associated with the electronic transaction;
 - [1.5] receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;
 - [1.6] subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;
 - [1.7.1] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
 - [1.7.2] performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
 - [1.7.3] determining, based at least in part on the captured biometric information, that the user is alive; and
 - [1.8] based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and
 - [1.9] a memory coupled to the processor and configured to provide the processor with instructions.

'656 Patent, claim 1

Claim 1 of '010 Patent

- [1.0] A system, comprising:
 - [1.1] one or more processors configured to:
 - [1.2] receive a virtual likeness of a face of an account holder; associate, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;
 - [1.3] render, in an interface, the virtual likeness of the face of the account holder;
 - [1.4] render a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;
 - [1.5] receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;
 - [1.6] capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
 - [1.7] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
 - [1.8] based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information, complete the electronic transaction; and
 - [1.9] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

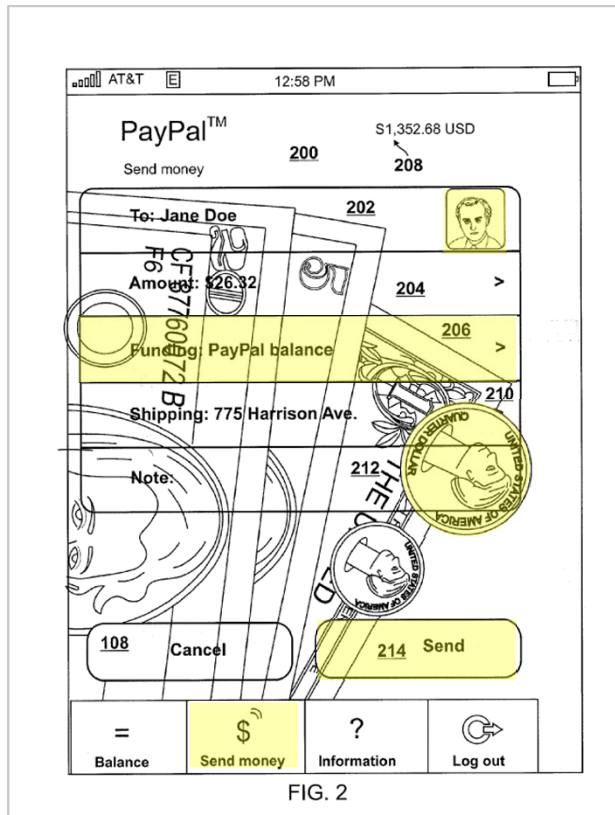
'010 Patent, claim 1

Discussion Roadmap

- Ground 1:
 - POSITA would have combined Stone, Hoyos, and Varghese (Slides 9-24)
 - Limitations [1.2] and [1.9] (slides 26-31)
 - Claims 5, 8, 14, and 17 (slides 33-37)
-
- Ground 2: (slides 39-45)
 - POSITA would have combined Stone and Guidance.
-
- Grounds 3 and 4: (slides 47-50)
 - POSITA would have combined Stone-Hoyos-Varghese and Stone-Guidance with Borovsky
-

Prior Art: Stone

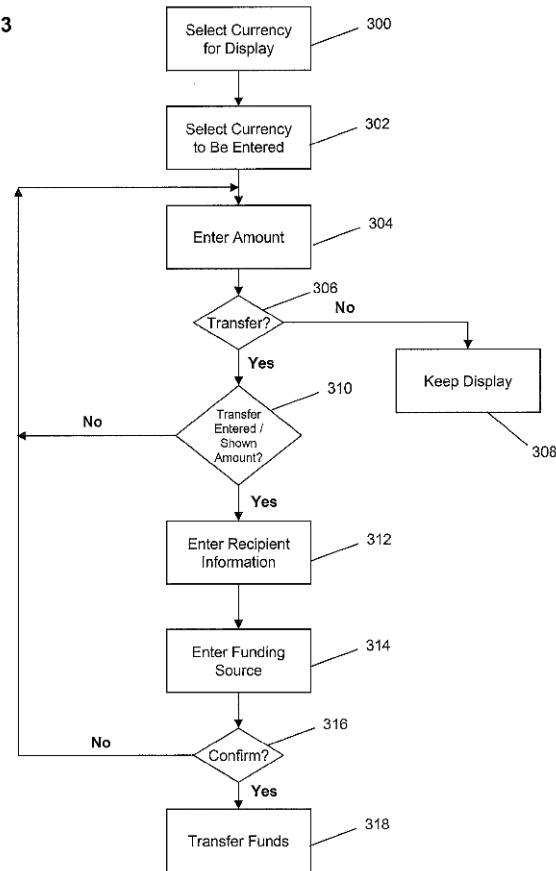
Display:



(Stone) APPL-1008, FIG. 2; Pet. 8.

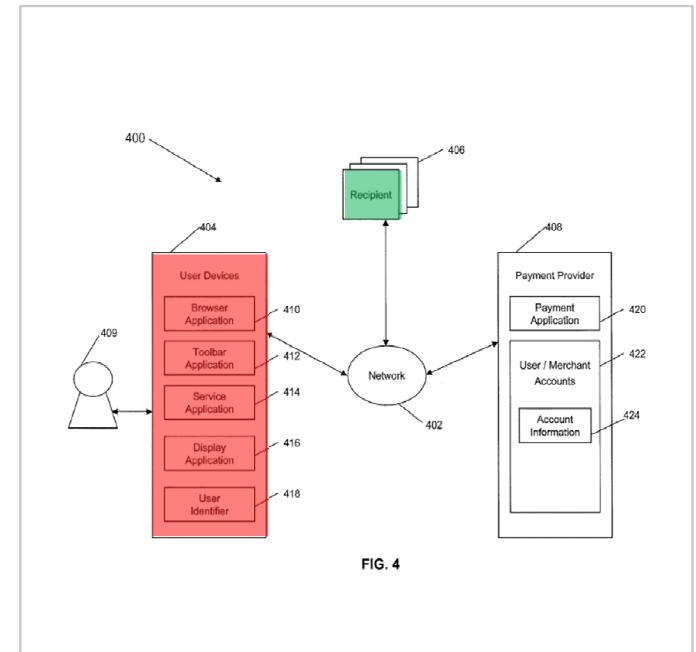
Financial Transaction:

FIG. 3



(Stone) APPL-1008, FIG. 3; Pet. 13-14.

System:



“recipient devices 406 may be the same or have the same basic features as user device 404”
(Stone) APPL-1008, FIG. 4, [0046]; Pet. 27-28.

Prior Art: Hoyos

Need of Authentication in Financial Transactions:

[0009] However, in the field of authentication of financial transactions, high levels of accuracy and speed are critical. For example, to authenticate a banking transaction, there is high motivation for an imposter to try to spoof the system and yet the financial institution would require a fast authentication process and a low rate of false rejects or denials. In this field, even a small percentage of rejections of authentications can result in an enormous number of unhappy customers, simply because of the huge number of transactions. This has prevented banks from using certain biometrics.

Authentication with accuracy, speed, and against spoofing using a combination of biometric match and liveness:

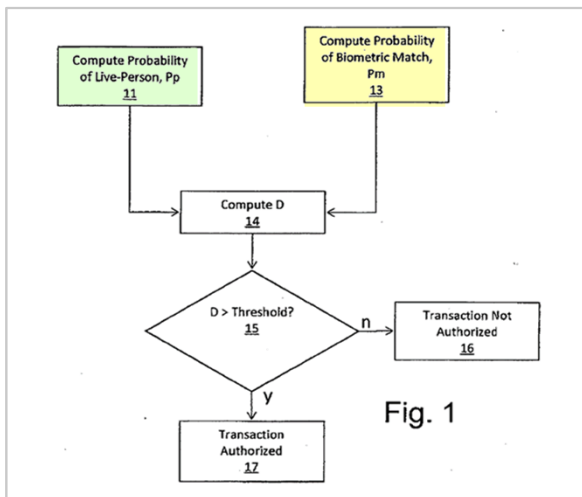


Fig. 1

(Hoyos) APPL-1013, [0009], [0011], [0029], FIG. 1; Pet., 8, 9, 10.

Problem of spoofing and live-person solution:

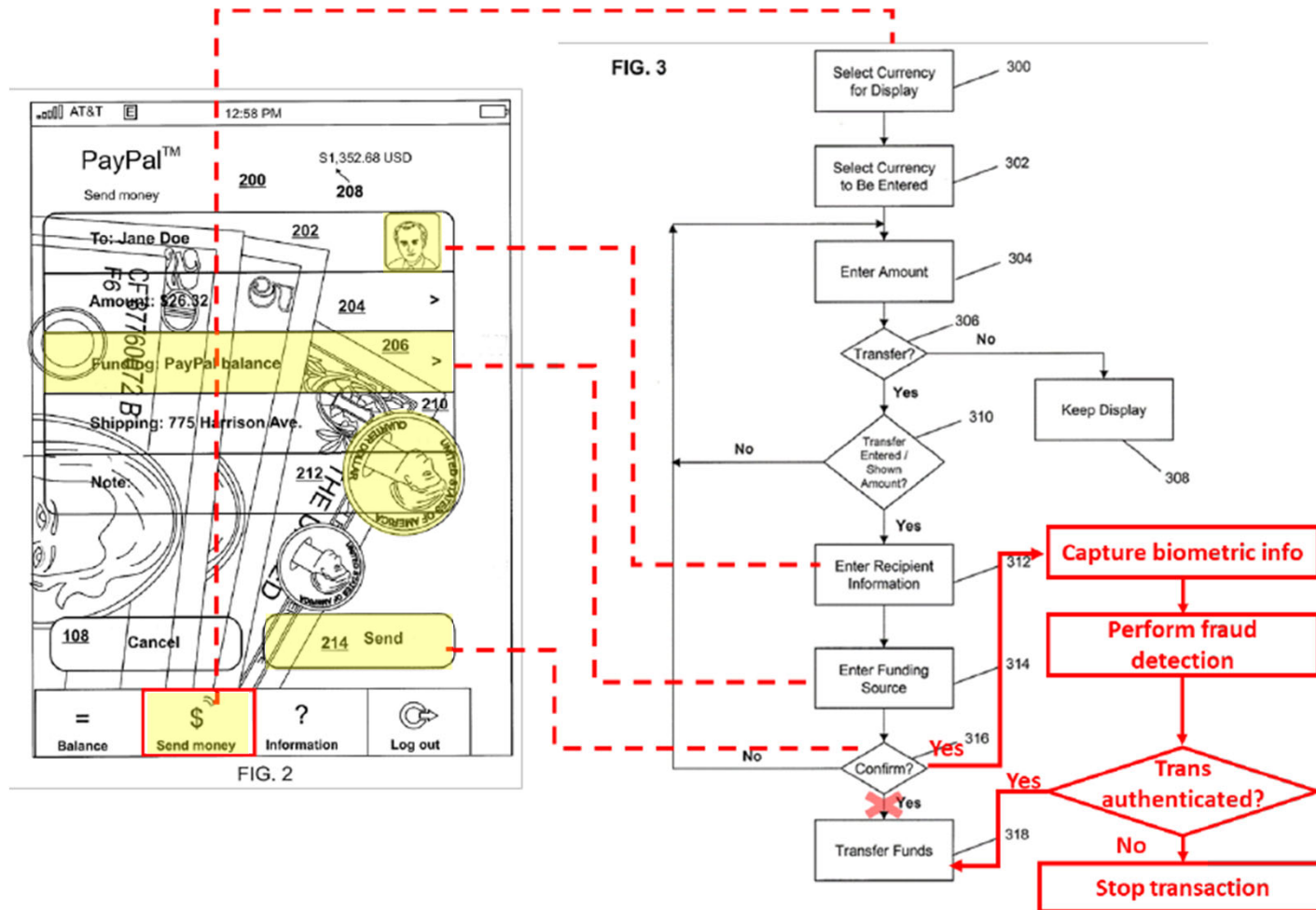
[0011] One problem faced by biometric recognition systems involves the possibility of spoofing. For example, a life-sized, high-resolution photograph of a person may be presented to an iris recognition system. The iris recognition systems may capture an image of this photograph and generate a positive identification. This type of spoofing presents an obvious security concern for the implementation of an iris recognition system. One method of addressing this problem

[0012] In biometric recognition systems using fingerprint, finger vein, palm vein, or other imagery, other methods of determining whether spoofing is being attempted use temperature or other measures of liveness, the term liveness being used herein for any step or steps taken to determine whether the biometric data is being acquired from a live human rather than a fake due to a spoof attempt. More specifically however, in this invention, we define probability of liveness as the probability that biometric data has been acquired that can be used by an automatic or manual method to identify the user.

Advantages:

[0029] A special advantage of this method and system is that by combining in one algorithm the live-person result with the match result, a fraudulent user does not know whether he or she was authorized or declined as a result of a bad or good match, or because the system has captured excellent live-person data that can be used for prosecution or at least embarrassing public disclosure. The system results in a large deterrent since in the process of trying to defeat a system, the fraudulent user will have to present some live-person data to the system and they will not know how much or how little live-person data is required to incriminate themselves. The fraudulent user is also not able to determine precisely how well their fraudulent methods are working, which takes away the single most important tool of a fraudster, i.e., feedback on how well their methods are working. At best, they get feed-

POSITA Would Have Combined Stone with Hoyos



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

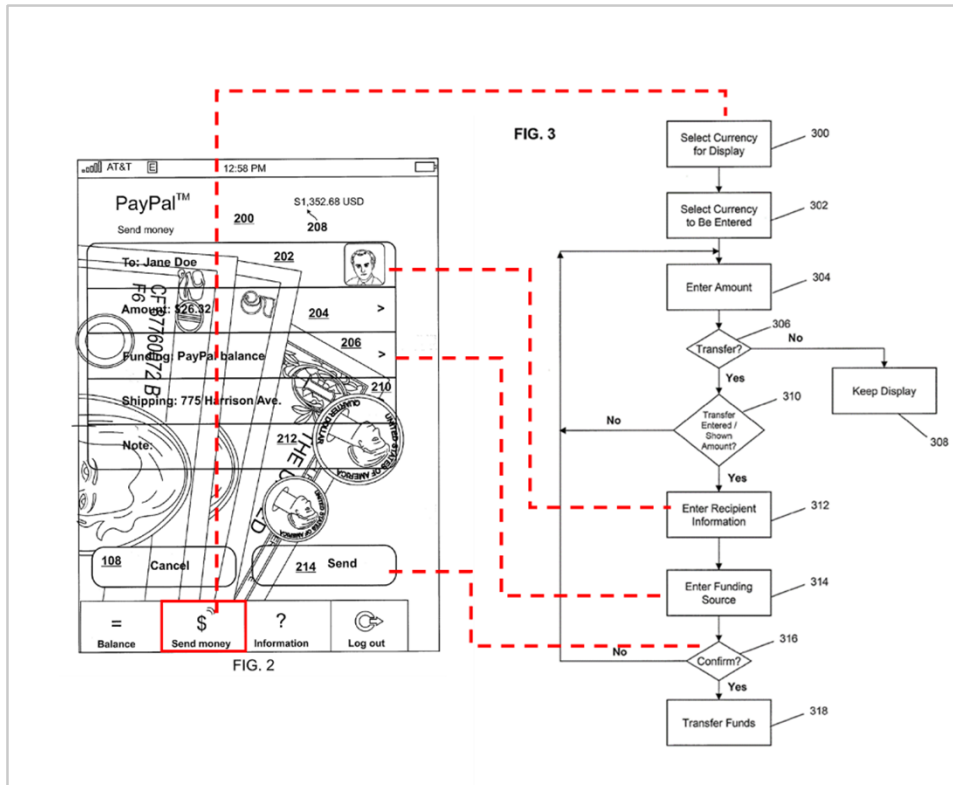
(Jones Decl.) APPL-1003, ¶¶ 59-68; (Stone) APPL-1008, FIGS. 2 and 3; (Hoyos) APPL-1013, FIG. 1, [0017]; Pet., 17.

Petitioner Has Established Motivation to Combine Stone with Hoyos Under *KSR*.

✓	“need or problem known in the field” <i>KSR</i>, 127 S.Ct. at 1742	Pet., 16 (“financial transactions of Stone had a <u>need</u> for authentication including fraud detection (e.g., with higher levels of security for some transactions)”); (Jones Decl.) APPL-1003, ¶61; (Hoyos) APPL-1013, [0009], [0011]; (Varghese) APPL-1010, [0148]; (Carter) APPL-1016, FIG. 3, [0073]; (Guidance) APPL-1037, 1; (Oracle-Bharosa Acquisition Announcement) APPL-1022, 1.
✓	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 15 (“benefits of <u>improved fraud resistancy</u> by addressing <u>spoofing</u> and achieving ‘<u>improved deterrent against attempted fraudulent transactions</u>, and decreased rejection of valid customers’ as taught by Hoyos”); APPL-1003, ¶¶59-68; (Hoyos) APPL-1013, [0015], [0017]-[0022], [0024], [0026], [0027], [0029]. Pet., 16 (“<u>proactively detect and prevent fraud</u>” driven by regulatory mandates such as FFIEC); (Oracle-Bharosa Acquisition Announcement) APPL-1022, 1; (Guidance) APPL-1037, 1; APPL-1003, ¶61.
✓	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 17-21 (“A POSITA would have <u>reasonably expected to succeed in configuring Stone-Hoyos, since the implementation of Hoyos’ biometric authentication in Stone would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date.</u>”) (Jones Decl.) APPL-1003, ¶¶66-67, (Carter) APPL-1016, [0040], [0042] [0076]; (Mardikar) APPL-1015, FIG. 3, 4:4-10; (Bhargav-Spantzel) APPL-1038, 64.

Stone Had a Need for Authentication for Financial Transactions.

- **Stone explicitly describes transfer funds in financial transactions.** (Stone) APPL-1008, [0001]-[0004]; (Jones Decl.) APPL-1003, ¶53; Pet. 13.
- **Stone explicitly describes authentication for financial transaction, discussing e.g. “user name, password,” “biometric id,” “security information.”** Preliminary Reply, 3; (Stone) APPL-1008, [0045].
- **Stone’s need is consistent with the well-known knowledge of the need for authentication for financial transactions.** APPL-1003, ¶61; (Hoyos) APPL-1013, [0009], [0011]; (Varghese) APPL-1010, [0148]; (Carter) APPL-1016, FIG. 3, [0073]; Pet. 16.



[0045] User device 408 may include one or more user identifiers 418, which may be implemented, for example, as operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers. User identifier 418 may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.). In various implementations, user identifier 418 may be passed with a user money transfer request to payment provider server 408, and user identifier 418 may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408.

(Stone) APPL-1008, FIGS. 2 and 3; Pet. 14; (Jones Decl.) APPL-1003, ¶56. (Stone) APPL-1008, [0045]; Pet. 13; (Jones Decl.) APPL-1003, ¶53.

Undisputed that a Need for Authentication for Financial Transactions was Well-Known in the Art

On August 8, 2001, the FFIEC agencies¹ (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;² increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

(FFIEC 2005Guidance) APPL-1037, 1; Pet. 16.

[0148] It should also be appreciated that the user or service provider may request further authentication during the course of a valid already-authenticated session based on, e.g., the transaction being requested. For example, a bank or other financial institution may wish to invoke a higher security authentication interface during a session before transactions over a certain amount are sent to the server. The systems and methods of the present invention can be invoked to provide for such authentication.

(Varghese) APPL-1010, [0148]; Pet. 16.

[0073] If the transaction matches the preferences, the transaction must then be authenticated before proceeding. At step 204, the necessary authentication level is determined based on the transaction criteria. As stated above, different authentication levels may be necessary for different transactions, based on factors such as value and type of transaction, as well as other factors. Once the necessary authentication level is determined, authentication is performed using one or more of the various authentication methods 205, including fingerprint validation 205A, PIN validation 205B, voice biometric validation 205C, facial recognition validation 205D, or GPS location validation 205E, each described above. The authentication is performed using authentication data 206 stored on the device 101. It is understood that different authentications may be used in other embodiments.

(Carter) APPL-1016, FIG. 3, [0073]; Pet. 16.

Hoyos's Techniques to Improve Authentication Would Improve Authentication for Financial Transactions in Stone in the Same Way

- **Hoyos's known biometric techniques have been used to improve authentication for financial transactions.**
Pet. 16; (Jones Decl.) APPL-1003, ¶62; (Hoyos) APPL-1013, [0024], [0026], [0027], [0029].
- **Hoyos's known techniques would improve similar financial transactions in Stone in the same way, using the known biometric techniques according to Hoyos' teachings.**
Pet. 17-21; (Jones Decl.) APPL-1003, ¶¶ 65-68, 103; (Hoyos) APPL-1013, [0015]; (Stone)APPL-1008, [0004].

“There is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’”

Intel Corp. v. PACT XPP Schweiz AG, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) (citations omitted) (quoting *KSR*, 550 U.S. at 417; *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 799–800 (Fed. Cir. 2021)); Inst. Dec. 64-65.

PO's Arguments are Contrary to the Record and the Law

PO Response Arguments:

- “Petitioner’s explanation for the alleged motivation to combine is conclusory.” POR, 16.
- “Stone is not analogous art” because “Stone is not concerned with payment processing and does not even recognize payment fraud as a problem needing to be solved.” POR, 22-23.
- “Stone and Hoyos teach away from each other and are incompatible because they are directed to different computing environments,” “Stone requires a client-server structure,” and “Hoyos’s disclosed authentication methods are employed locally on the device, with no mention of a server structure.” POR, 24.

Petitioner’s Reply:

- The reasons to combine are supported by Dr. Jones’ detailed explanation and numerous references, including references from PO’s own expert Dr. Goodrich. Pet. 15-21; Reply, 29; APPL-1003, ¶¶59-68; (Hoyos) APPL-1013, [0015], [0017]-[0022]; (Varghese) APPL-1010, [0148], FIG. 14, [0097]-[0099], TABLE 10; (Carter) APPL-1016, FIG. 3, [0073]; (Guidance) APPL-1037, 7-14; (Mardikar) APPL-1015, FIG. 4; (Bansal) APPL-1035, 4:60-62; 4:66-67.
- Stone is analogous art. Like ‘656 Patent, Stone
 - addresses the same problem of making the transaction seem “more concrete” by showing “actual currency” on display. (‘656 Patent) APPL-1001, 4:28–30, 4:62–67, 5:16–18; (Stone) APPL-1008 ¶¶ 6, 8, 10–11, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; Reply, 5.
 - discloses secure transactions with multi-factor authentication. Prelim. Reply, 3.
 - discloses user interface art (e.g., dragging icon for payment), which is integral to fraud detection in financial transactions. Prem. Reply, 4.
- Stone’s client-server model and Hoyos’ authentication methods are complementary. A POSITA would adapt Hoyos’ biometric methods to function within Stone’s system (either on the client or on a server), achieving secure authentication without undermining the system’s architecture. Pet., 16-20; APPL-1003, ¶¶67-68; Reply, 6-7; APPL-1055, 2.

Undisputed that Authentication in Client-Server System was Well-Known.

PO's expert, Dr. Goodrich, acknowledges that authentication for client-server system was well-known, with “two broad approaches” for authentication: (1) at a remote server; and (2) locally “at the client end [which m]ost of the recent work has focused on”):

There is a huge literature on biometric authentication, and we briefly focus here on the work most relevant to our paper. There are two broad approaches: The one where the comparison is done at the remote server, and the one where the comparison is done at the client end (the portable device where the biometric measurement is done). Most of the recent work has focused on the second category, ever since the landmark paper of Davida et al. [9] proposed that comparisons be done at the client end (although their scheme is also useful in the first case, of remote comparison at the server end). Many other papers (e.g., [4,

(Goodrich C101) APPL-1055, 2; Reply, 15.

POSITA “has good reason to pursue the known options within his or her technical grasp” where there are “there are a finite number of identified, predictable solutions” for solving the design need.

KSR Intern. Co. v. Teleflex Inc., 127 S.Ct. 1727, 1732.

PO does not (and cannot) Establish Teaching Away.

“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.” *Ricoh Co., Ltd. v. Quanta Computer Inc.*, 550 F.3d 1325, 1332 (Fed.Cir.2008) (quoting *In re Kahn*, 441 F.3d 977, 990 (Fed.Cir.2006)). A reference does not teach away, however, if it merely expresses a general preference for an alternative invention but does not “criticize, discredit, or otherwise discourage” investigation into the invention claimed.

Reply, 6-7; *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009); *see also* *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

Prior Art: Varghese

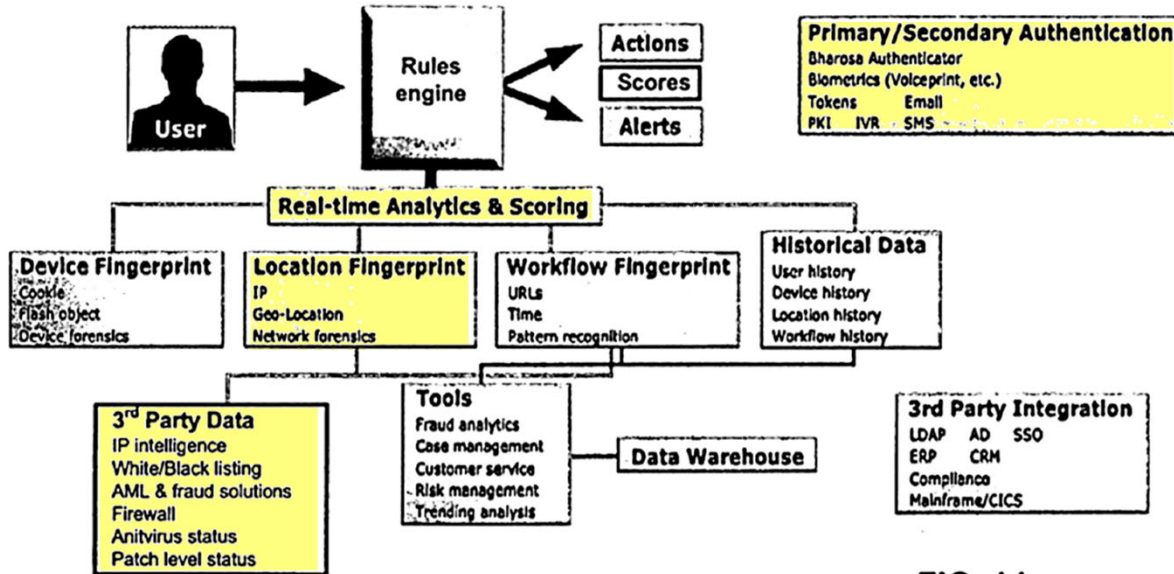


FIG. 14

Varghese describes multifactor real-time authentication during the course of an already authenticated session based on the transaction.

(Varghese) APPL-1010, FIG. 14; Pet. 10.

[0148] It should also be appreciated that the user or service provider may request further authentication during the course of a valid already-authenticated session based on, e.g., the transaction being requested. For example, a bank or other financial institution may wish to invoke a higher security authentication interface during a session before transactions over a certain amount are sent to the server. The systems and methods of the present invention can be invoked to provide for such authentication.

(Varghese) APPL-1010, [0148]; Pet. 24.

[0109] Business policies generally include rules (referred to as “transaction rules”) that evaluate parameters of individual in-session transactions for the likelihood of fraud or malicious intent. Accordingly, business policies are generally application during post-authentication are generally specific to the field or to the business of the service provider and service provider application. For example, in a banking application, specific transaction rules can be directed to specific banking transactions, e.g. bill pay, transfer funds, and the like. Transaction models can be used in conjunction with security rule, e.g. don’t allow (or challenge user for) money transfer request from an international IP address. Business policies can be shared by different service providers in a particular field, or can created and customized for a specific service provider.

(Varghese) APPL-1010, [0109]; Pet. 41.

Petitioner has Established Motivation to Combine Stone, Hoyos with Varghese Under *KSR*.

	“need or problem known in the field” <i>KSR</i>, 127 S.Ct. at 1742	Pet., 16 (“financial transactions of Stone had a need for authentication including fraud detection (e.g., with <u>higher levels of security for some transactions</u>)”); (Jones Decl.) APPL-1003, ¶61; (Hoyos) APPL-1013, [0009], [0011]; (Varghese) APPL-1010, [0148]; (Carter) APPL-1016, FIG. 3, [0073]; (Guidance) APPL-1037, 1; (Oracle-Bharosa Acquisition Announcement) APPL-1022, 1.
	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 21-22 (“multifactor real-time authentication” for “improved security for financial transactions”); 22-23 (“detecting and preventing <u>access attempts from locations commonly associated with cyber threats</u>, providing cross-checking with a user location for a transaction request, and providing additional security without significant additional inconvenience to the user”). Pet., 18, 24 (“A POSITA would have understood that, compared to the alternative design choice of using previously captured authentication data as the input data for transaction authentication, performing <u>real-time authentication using authentication data captured after and in response to user transaction request confirmation</u> had various benefits with improved security.”).

Petitioner has Established Motivation to Combine Stone, Hoyos with Varghese Under *KSR*.

	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 23-26, 45 (“A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese to leverage Varghese’s multifactor real-time authentication functionality since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date”); APPL-1003, ¶¶72-77; (Carter) APPL-1016, [0036]; (Guidance) APPL-1037, 7-12.
---	--	---

PO's Arguments are Contrary to the Record and the Law

PO Response arguments:

- Varghese amplifies the disconnect between Stone and Hoyos regarding the server and client distinction. Varghese, like Stone, envisions a client-server structure.
- The hardware-based biometrics collection and authentication techniques described in Hoyos do not support Varghese's stated goal of providing a "purely software based solution to identify theft" (i.e., fraud detection).
- Varghese teaches away from applying a location check as a final step of fraud detection analysis.

POR, 27-31.

Petitioner's Reply:

- The asserted "server and client distinction" fails for the same reasons discussed regarding Stone and Hoyos.
- Varghese describes a "purely software based solution to identify theft that does not require hardware devices to be issued and maintained", which does not exclude using biometric sensors. (Varghese) APPL-1010, [0022], [0079] (explicitly describes the use of sensor-based biometrics including "obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like)." Reply 8.
- Varghese describes transaction authentication ("post-authentication") using real-time location authentication. Pet. 11; Reply, 9-10.

Varghese Describes Transaction Authentication (“Post-authentication”) Using Real-Time Location

46. As shown in FIG. 14 of Varghese above, Varghese describes performing real-time multi-factor authentication (e.g., location authentication using “Geo-Location” by user device IP address and voice authentication (e.g., using “Biometrics (Voiceprint, etc.)”) for improved fraud analysis. (Varghese) APPL-1010, FIG. 14. Varghese describes fraud analytics implementing various policies, which “can be enforced during pre-authentication, for example when a user is being authenticated, or during post-authentication, for example when a user is making transaction requests.” (Varghese) APPL-1010, [0097]-[0099]; *see also* (Varghese) APPL-1010, [0081], [0084], [0088], [0140] (“Geolocation by IP address is a technique of determining the geographic latitude and longitude corresponding to a user by comparing the user’s IP address with known locations of other nearby servers and routers”), [0142], claim 31.

(Jones Decl.) APPL-1003, ¶46.

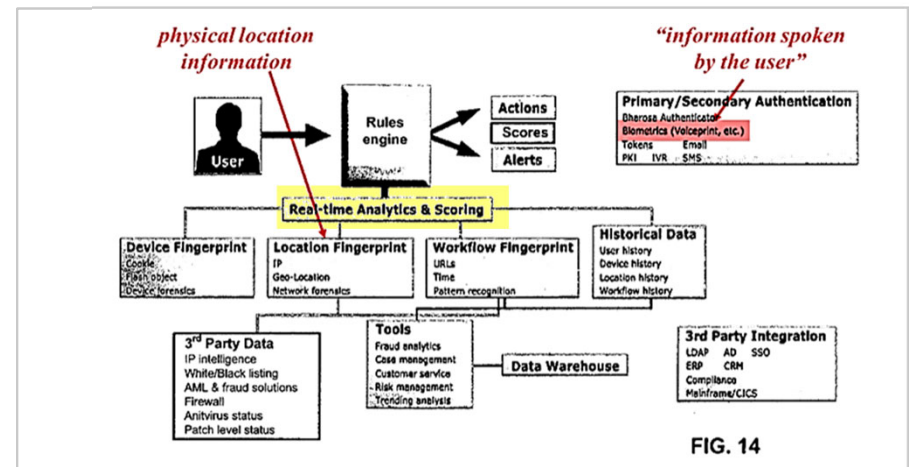


FIG. 14

(Varghese) APPL-1010, FIG. 14; Pet., 45.

[0148] It should also be appreciated that the user or service provider may request further authentication during the course of a valid already-authenticated session based on, e.g., the transaction being requested. For example, a bank or other financial institution may wish to invoke a higher security authentication interface during a session before transactions over a certain amount are sent to the server. The systems and methods of the present invention can be invoked to provide for such authentication.

(Varghese) APPL-1010, [0148]; Pet. 45.

Undisputed POSITA's Knowledge that "Real-Time" Authentication Includes Both Real-Time Capture and Real-Time Analysis of Data.

114. A POSITA would have understood "real-time" authentication as described in Varghese includes both real-time capture and real-time analysis of authentication data, which provides more accurate fraud analysis by using more accurate, real-time data. (Carter) APPL-1016, [0043] (describing real-time GPS capture for GPS location authentication, where "[a high value] transaction will be prevented unless the person is identified to be a specific location. For example, a mortgage may be prevented from closing if the person is not in a bank" as verified by GPS location); [0044] (describing obtaining "the location of the transaction" to determine "the level of authentication"); (Bansal) APPL-1035, 4:60-62 (describing real-time authentication data capture (e.g., real-time voice print authentication) has the benefit to "avoid imposters from communicating based on stolen biometric data"), 4:66-67 (describing using various "real-time biometric data such as voice prints, retina scans for fingerprint recordings"); (Guidance) APPL-1037, 10 (describing "live scan process of the biometrics technology" for authentication)).

(Jones Decl.) APPL-1003, ¶114 (citing (Carter) APPL-1016, [0043]-[0044], (Bansal) APPL-1035, 4:60-62 .

Undisputed well-known knowledge

- **real-time authentication includes both real-time capture and real-time analysis.**
- **benefits of real-time authentication include providing more accurate fraud analysis and avoid imposters.**
- **real-time authentication was used prior to closing a transaction.**

Discussion Roadmap

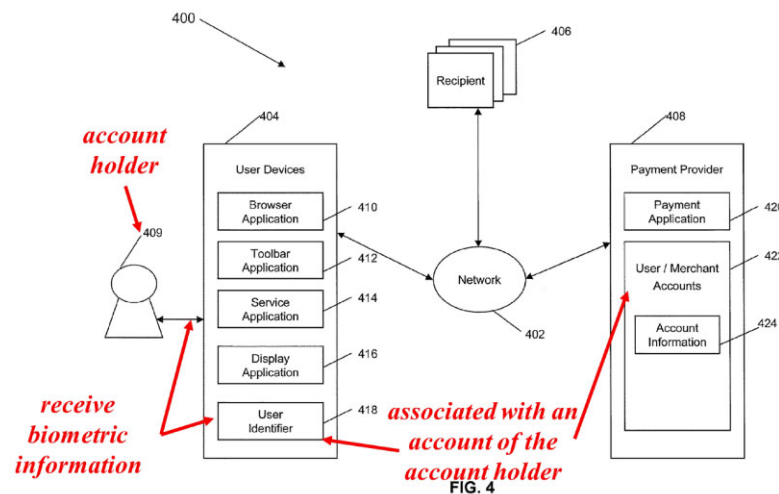
- Ground 1:
 - POSITA would have combined Stone, Hoyos, and Varghese (Slides 9-24)
 - Limitations [1.2] and [1.9] (slides 26-31)
 - Claims 5, 8, 14, and 17 (slides 33-37)
 - Ground 2: (slides 39-45)
 - POSITA would have combined Stone and Guidance.
 - Grounds 3 and 4: (slides 47-50)
 - POSITA would have combined Stone-Hoyos-Varghese and Stone-Guidance with Borovsky
-

Limitation [1.2]

[1.2] [a processor configured to:] receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;

Ground 1 Renders Obvious [1.2] “Store...the Received Biometric Information, Wherein the Biometric Information Is Associated With an Account of the Account Holder”

Stone describes storing “biometric id” in a data store of user device, wherein the stored “biometric id” (a user attribute of user identifier 418) is associated with an account (account 422) of the account holder (user 409).



APPL-1008, FIG. 4, annotated

[0045] User device 408 may include one or more user identifiers 418, which may be implemented, for example, as operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers. User identifier 418 may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.). In various implementations, user identifier 418 may be passed with a user money transfer request to payment provider server 408, and user identifier 418 may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408.

(Stone) APPL-1008, FIG. 4; Pet. 32

(Stone) APPL-1008, [0045]; Pet. 31.

Ground 1 Renders Obvious [1.2] “Store...the Received Biometric Information, Wherein the Biometric Information is Associated With an Account of the Account Holder”

[0045] User device 408 may include one or more user identifiers **418**, which may be implemented, for example, as operating system registry entries, cookies associated with browser application **410**, identifiers associated with hardware of user device **404**, or various other appropriate identifiers. User identifier **418** may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.). In various implementations, user identifier **418** may be passed with a user money transfer request to payment provider server **408**, and user identifier **418** may be used by payment provider server **408** to associate user **409** with a particular user account maintained by payment provider server **408**.

(Stone) APPL-1008, [0045]; Pet. 31.

associated with a user account

User Identifier 418

User Name

Password

Photograph Image

Biometric id

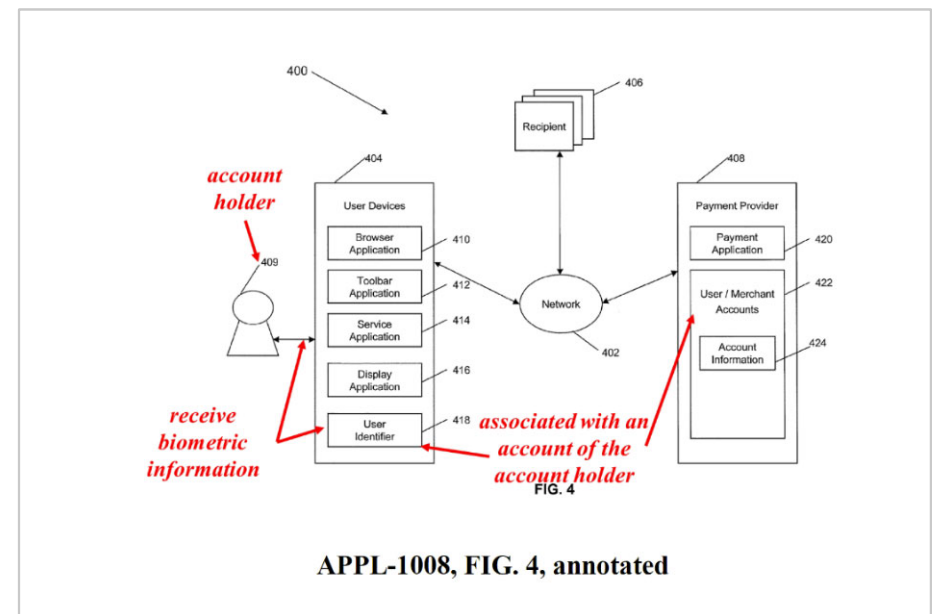
used by payment provider in context of money transfer request to associate user 409 with a user account.

PO's Sur-Reply Arguments are Contrary to Record

- ✗ “Stone does not disclose any association between user identifier 418 (what Petitioner identifies as the user biometric) and user account 422 (account of an account holder) that occurs on the user device 404. The only association of user identifier 418 with an account occurs on the payment provider server 408.... Ex. 1008 at [0045]-[0046].” (Sur-Reply, 11).
- ✗ “POSITA would not have been motivated to implement local authentication as taught by Hoyos on Stone’s server structure, given wide variance among user devices.” (Sur-Reply, 13)

[0045] User device 408 may include one or more user identifiers 418, which may be implemented, for example, as operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers. User identifier 418 may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.). In various implementations, user identifier 418 may be passed with a user money transfer request to payment provider server 408, and user identifier 418 may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408.

(Stone) APPL-1008, [0045]; Pet. 31.



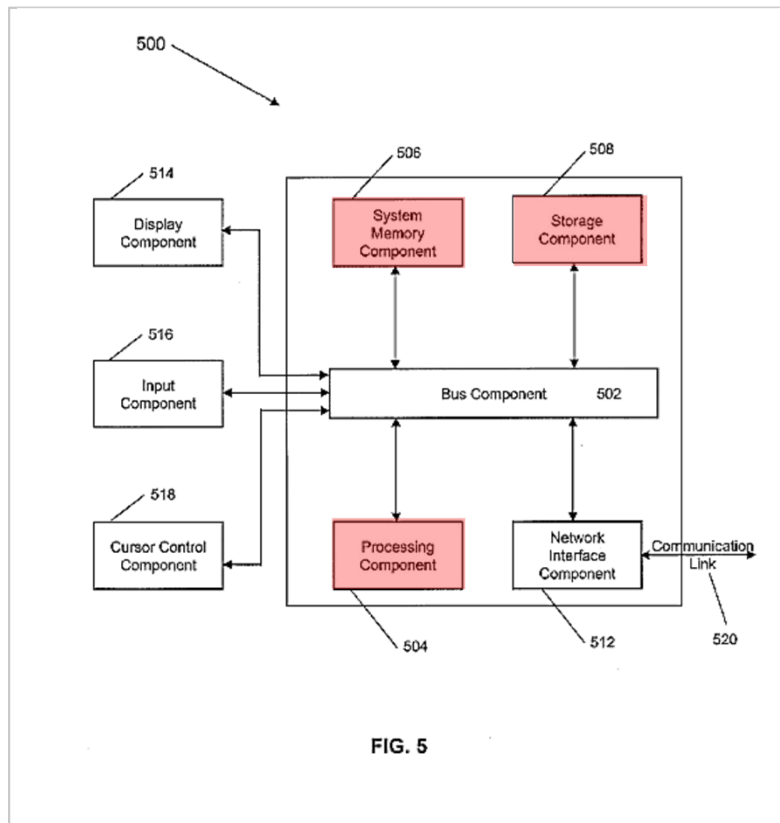
(Stone) APPL-1008, FIG. 4; Pet. 32.

Limitation [1.9].

[1.9] a memory coupled to the processor and configured to provide the processor with instructions.

Ground 1: Stone in view of Hoyos and Varghese Renders Obvious [1.9].

[1.9] a memory coupled to the processor and configured to provide the processor with instructions.



(Stone) APPL-1008, FIG. 5; Pet. 51-52.

[0050] In accordance with embodiments of the invention, system 500 performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in system memory component 506. Such instructions may be read into system memory component 506 from another computer readable medium, such as static storage component 508. These can include instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc. In other embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention.

(Stone) APPL-1008, [0050]; Pet. 51-52.

Discussion Roadmap

- Ground 1:
 - POSITA would have combined Stone, Hoyos, and Varghese (Slides 9-24)
 - Limitations [1.2] and [1.9] (slides 26-31)
 - Claims 5, 8, 14, and 17 (slides 33-37)
 - Ground 2: (slides 39-45)
 - POSITA would have combined Stone and Guidance.
 - Grounds 3 and 4: (slides 47-50)
 - POSITA would have combined Stone-Hoyos-Varghese and Stone-Guidance with Borovsky
-

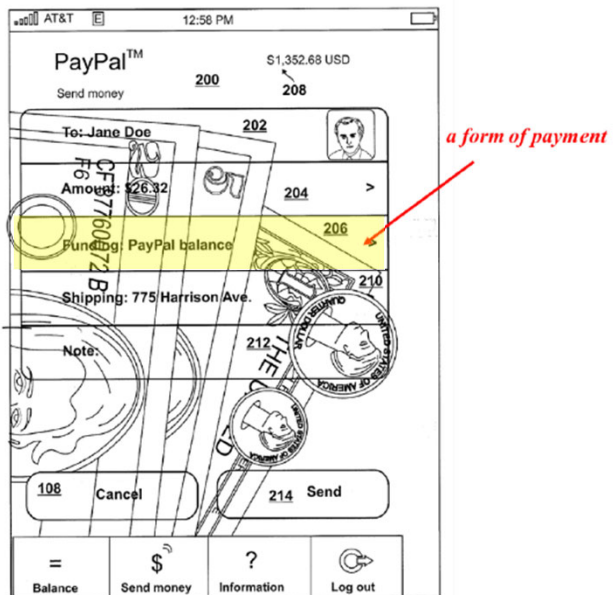
Claims 5 and 14

Claim 5. The system of claim 1 wherein the transaction icon comprises a graphical representation of a payment form.

Claim 14. The method of claim 10 wherein the transaction icon comprises a graphical representation of a payment form.

Ground 1: Stone in view of Hoyos and Varghese Renders Obvious Claims 5 and 14

[5.0/14.0] The system of claim 1/method of claim 10 wherein the transaction icon comprises a graphical representation of a payment form.



[0038] In other embodiments, the display on a device may show a financial instrument, such as a specific type of credit card, bank card, or debit card. These may or may not be the selected funding sources. Once selected or swiped, the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a card or no visual at all. The visual image of the card could be shown in the background and relevant information, such as balance, past transactions, current transaction, amount, etc., can be shown on the foreground.

(Stone) APPL-1008, FIG. 2; Pet. 53-54.

(Stone) APPL-1008, FIG. 2; Pet. 53.

Dr. Jones Explains the Benefits of Using a Graphical Representation of a Payment Form.

151. To the extent that Stone does not explicitly describe that the funding source selection interface includes an icon representing a form of payment, it would have been obvious to a POSITA to implement the funding source selection using an icon with the visual representation of the payment (e.g., a PayPal card, Visa, MC, AMEX) for improved visual presentation. (Stone) APPL-1008, [0004] (recognizing that “icon” and “button” are alternative design choices, stating that “[t]he consumer typically clicks on an icon or button to make the transfer.”); (Stone) APPL-1008, [0038] (describing using icons of the funding sources for improved visual presentation, stating “the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a card or no visual at all.”).

Benefit of Improved Visual Presentation.

Graphical Representations of Particular Forms of Payment.

(Jones Decl.) APPL-1003, ¶151; Petition, 54.

Claims 8 and 17

Claim 8. The system of claim 1 wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.

Claim 17. The method of claim 10 wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.

Ground 1 Renders Obvious Claims 8 and 17

Undisputed evidence that an avatar was a well-known alternative design choice of pictures for a user icon.

Mobile device 104 can display (228) the notification received from server 112. Displaying the notification can include displaying a match score between mobile device 104 and mobile device 106, as well as a providing a user name or a profile image set up for mobile device 106. For example, a profile picture or avatar of Baker can be displayed on mobile device 104.

(Chatterjee) APPL-1009, 9:30-35; (Jones Decl.) APPL-1003, ¶106; Pet. 56-57.

POSITA “has good reason to pursue the known options within his or her technical grasp” where there are “there are a finite number of identified, predictable solutions” for solving the design need.

KSR Intern. Co. v. Teleflex Inc., 127 S.Ct. 1727, 1732.

Undisputed evidence that an avatar has the benefits of providing an online identity that balances personal expression and privacy.

Increasingly, social system designers are introducing avatars as the new forum for identity construction in online environments, a feature users have welcomed with enthusiasm. Following Yahoo’s launch of Yahoo! Avatars, 7 million users personalised an avatar for display within their profiles e.g. Yahoo! 360°, Yahoo! Answers, Yahoo! Messenger (Hemp, 2006). Likewise, four million users created an avatar after the facility (called ‘weemee’) was introduced to the chat system ‘Windows Live Messenger’.¹ This rapid uptake of avatars is not surprising; while avatars maintain users’ privacy, they give expressive freedom over an otherwise static online identity. In an illustrative example, V-Chat, a virtual chat-room, allowed users to either design their own avatar, which was particularly time demanding, or to select from already-made options. In general, V-Chat users spurned the latter option, instead taking the time to create unique representations so that they “didn’t look like others” (Cheng et al., 2002).

(Vasalou) APPL-1047, 801; (Jones Decl.) APPL-1003, ¶106; Pet. 56.

Discussion Roadmap

- Ground 1:
 - POSITA would have combined Stone, Hoyos, and Varghese (Slides 9-24)
 - Limitations [1.2] and [1.9] (slides 26-31)
 - Claims 5, 8, 14, and 17 (slides 33-37)
 - Ground 2: (slides 39-45)
 - POSITA would have combined Stone and Guidance.
 - Grounds 3 and 4: (slides 47-50)
 - POSITA would have combined Stone-Hoyos-Varghese and Stone-Guidance with Borovsky
-

Prior Art: FFIEC Guidance

Need and benefits for multi-factor real-time authentication:

FFIEC Guidance Authentication in an Internet Banking Environment

FIL-103-2005
October 12, 2005

Summary:

The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance, "Authentication in an Internet Banking Environment." For banks offering Internet-based financial services, the guidance describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using the on-line products and services. Examiners will review this area to determine a financial institution's progress in complying with this guidance during upcoming examinations. Financial Institutions will be expected to achieve compliance with the guidance no later than year-end 2006.

Highlights:

- Financial institutions offering Internet-based products and services should use effective methods to authenticate the identity of customers using those products and services.
- Single-factor authentication methodologies may not provide sufficient protection for Internet-based financial services.
- The FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.
- Risk assessments should provide the basis for determining an effective authentication strategy according to the risks associated with the various products and services available to on-line customers.
- Customer awareness and education should continue to be emphasized because they are effective deterrents to the on-line theft of assets and sensitive information.

Existing authentication methodologies involve three basic "factors":

- Something the user *knows* (e.g., password, PIN);
- Something the user *has* (e.g., ATM card, smart card); and
- Something the user *is* (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out-of-band"⁵ controls for risk mitigation.

(Financial Institution Letters) APPL-1039, 1; Pet. 11.

**Multi-factor real-time
authentication:
more reliable and stronger
fraud deterrents**

(Guidance) APPL-1037, 3; Pet. 11.

Prior Art: FFIEC Guidance

Biometrics with tests for live person

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called “mug shot” environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Facial recognition techniques

- “tests for liveness, such as blinking eyes.”
- “reduces the chance that the person requesting access is using a photograph.”

(Guidance) APPL-1037, 11; Pet. 12, 71; APPL-1003, ¶¶ 230-231 (citing (Kollreider) APPL-1044, 2; (Hoyos) APPL-1013, FIGS. 2-4, claims 5-6).

Internet Protocol Address (IPA) Location and Geo-Location

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as “IP Intelligence.” The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user’s IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user’s location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

Techniques to determine where users are or conversely, where they are not.

- “real-time environment”
- “IP Intelligence”
- “Geo-location”

(Guidance) APPL-1037, 12; Pet. 70; (Jones Decl.) APPL-1003, ¶¶ 224-225.

Petitioner has Established Motivation to Combine Stone with FFIEC Guidance Under *KSR*.

 	“need or problem known in the field” <i>KSR</i>, 127 S.Ct. at 1742	Pet., 16 (“financial transactions of Stone had a <u>need for authentication including fraud detection (e.g., with higher levels of security for some transactions)</u>”); (Jones Decl.) APPL-1003, ¶61; (Hoyos) APPL-1013, [0009], [0011]; (Varghese) APPL-1010, [0148]; (Carter) APPL-1016, FIG. 3, [0073]; (Guidance) APPL-1037, 1; (Oracle-Bharosa Acquisition Announcement) APPL-1022, 1.
	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 62(“the <u>benefits of improved security and boosted customer confidence for service providers even not subject to FFIEC supervision, and the additional benefits of FFIEC compliance for federal supervised financial institutions.</u>”); (Jones Decl.) APPL-1003, ¶¶199.
	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 63 (“A POSITA would have reasonably expected to succeed in configuring Stone to implement the multifactor, real-time, risk-based authentication functionality taught by Guidance, since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date.”); (Jones Decl.) APPL-1003, ¶202 (citing (Financial Institution Letter) APPL-1039, 1; (Stone) APPL-1008, [0041]-[0042]).

Sur-Reply Mischaracterizes POSITA's Interest in the FFIEC Guidance.

First, Petitioner's claim that the record illustrates a POSITA's interest in the Guidance is unavailing. Pet. Reply, 25-26. For starters, the FFIEC's regulatory authority is limited to banks and financial institutions. Ex. 1037, 1. For the '656 Patent, a POSITA as defined in the Board's Institution Decision, has no credentials or affiliation with the banking industry. *See* Paper [10], 11-12. Further, Stone, Petitioner's primary reference, is assigned to eBay, which is not a bank or financial institution subject to the FFIEC's authority. The three patent disclosures Petitioner cites as referencing the Guidance are also all assigned to financial institutions or expressly reference compliance requirements of financial institutions. *See* Pet. Reply, 25; Ex. 1003, ¶ 50. And Petitioner's expert's personal knowledge of and testimony about the Guidance's "significance" is based on his work in standard setting organizations, which is far beyond a POSITA's limited work experience (bachelor's degree and two years' experience in development of biometric authentication techniques). Ex. 1049, 55:4-55:12 ("[T]hose of us in the standardization community paid great attention to it [FFIEC Guidance], so I've been familiar with it since.").

- **Sur-Reply incorrectly asserts that only a person in the bank industry would be interested in the Guidance.**
- **Sur-Reply improperly limits Dr. Jones's personal experience in the industry.**
- **Sur-Reply misrepresents supporting references presented by Petitioner.**

Sur-Reply, 18-19.

Oracle-Bharosa Acquisition Announcement Highlighted FFIEC as Driver for Authentication Solutions.

Even for service providers not regulated by FFIEC, FFIEC Guidance is a driver for “improved authentication technologies.” APPL-1003, ¶201; Pet. 62.

Online fraud has increased, causing users to lose confidence in web-based services and leading to significant impact to business. Driven by specific regulatory mandates such as FFIEC, PCI, and HIPAA, organizations are under pressure to proactively detect and prevent fraud and provide more granular reporting of their progress toward protecting the privacy of consumers. Bharosa provides key capabilities spanning strong authentication, mutual authentication, contextual authorization, proactive real-time risk monitoring and fraud detection, and real-time reporting and analysis. Their proven technology secures leading consumer web sites, including those of National City Bank, and 30 others, protecting over 25 million users. Bharosa’s products restore

(Oracle-Bharosa Acquisition Announcement) APPL-1022, 1; APPL-1003, ¶201; Pet. 62.

Sur-Reply Mischaracterizes POSITA's Interest in the FFIEC Guidance.

- **Dr. Jones explained that Guidance was valuable input from the financial community for security and biometrics technology.** APPL-1056, ¶ 48; Pet. 25-26.
- **Dr. Jones explained his own experience in the industry of biometric device providers.** APPL-1056, ¶ 49; Pet. 25-26.

standardization arena, and we in M1 and SC37 considered it carefully. It represented valuable input from the financial community on the requirements for biometric authentication of financial transactions, and standards for data storage and transmission, interoperability, API standardization and biometrics use were all developed with this Guidance in mind.

49. At Sagem Morpho, I was a supervisor to engineers who were POSITAs, and it was my own experience that the Guidance was within the interested subject matter of a POSITA. It was my personal experience that POSITAs in the engineering staff at Sagem Morpho were interested in the Guidance, and further used the Guidance as part of our approach of providing biometrics subsystems for use in financial applications. It was also my personal experience that POSITAs in the development staff of our parent company, SAGEM SA, who developed fingerprint sensors and biometric terminals, were interested in the Guidance.

Sur-Reply Mischaracterizes POSITA's Interest in FFIEC Guidance.

[PDF] Authentication in an internet banking environment

FFIE Council - Retrieved June, 2005 - financialbrowsers.com

... of Internet banking should have effective and reliable methods to authenticate customers. ... s overall strategy for Internet banking and electronic commerce services. The level of ...

☆ Save Cite Cited by 158 Related articles All 45 versions

(12) United States Patent Speyer et al.

(10) Patent No.: US 8,032,932 B2
(45) Date of Patent: Oct. 4, 2011

(54) SYSTEMS AND METHODS FOR PROVIDING SECURITY TOKEN AUTHENTICATION

(75) Inventors: Jerry Speyer, Tampa, FL (US);
Sandeep Nair, Riverview, FL (US);
Ricky Luo, Berkeley Heights, NJ (US)

(73) Assignee: Citibank, N.A., New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 544 days.

(21) Appl. No.: 12/196,526

(22) Filed: Aug. 22, 2008

(56) References Cited

U.S. PATENT DOCUMENTS

7,516,483 B2 *	4/2009	Brennan	726/9
2001/0045451 A1 *	11/2001	Tan et al.	235/375
2003/0191711 A1 *	10/2003	Jamison et al.	705/40
2004/0059952 A1 *	3/2004	Newport et al.	713/202
2004/0250118 A1 *	12/2004	Andreev et al.	713/201
2005/0033703 A1 *	2/2005	Holdsworth	705/67
2005/0149759 A1 *	7/2005	Vishwanath et al.	713/201
2005/0166263 A1 *	7/2005	Nanopoulos et al.	726/7
2007/0016943 A1 *	1/2007	M'Raihi et al.	726/9
2007/0022196 A1 *	1/2007	Agrawal	709/225
2007/0186106 A1 *	8/2007	Ting et al.	713/168
2008/0228653 A1 *	9/2008	Holdsworth	705/67
2009/0055907 A1 *	2/2009	Van Horn	726/6

* cited by examiner

Primary Examiner — Michael Simitoski

(74) Attorney, Agent, or Firm — Johnson & Associates

(12) United States Patent Colson

(10) Patent No.: US 8,239,677 B2
(45) Date of Patent: Aug. 7, 2012

(54) VERIFICATION AND AUTHENTICATION SYSTEMS AND METHODS

(75) Inventor: Christen J. Colson, Alpharetta, GA (US)

(73) Assignee: Equifax Inc., Atlanta, GA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 964 days.

(21) Appl. No.: 11/545,247

(22) Filed: Oct. 10, 2006

(12) United States Patent Stebila et al.

(10) Patent No.: US 8,776,176 B2
(45) Date of Patent: Jul. 8, 2014

(54) MULTI-FACTOR PASSWORD-AUTHENTICATED KEY EXCHANGE

(75) Inventors: Douglas J. Stebila, Waterloo (CA);
Poornaprajna V. Udupi, Sunnyvale, CA (US);
Sheueling Chang Shantz, Cupertino, CA (US)

(73) Assignee: Oracle America, Inc., Redwood Shores, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1288 days.

(21) Appl. No.: 12/143,964

(22) Filed: Jun. 23, 2008

OTHER PUBLICATIONS

Abdalla, Michel et al., "Strong Password-Based Authentication in TLS using the Three-Party Group Diffie-Hellman Protocol", International Journal of Security and Networks, http://www.inderscience.com/search/index.php?action=record&rec_id=13181&prevQuery=&ps=10&m=or, 2006, pp. 1-18.

Gennaro, Rosario et al., "A Framework for Password-Based Authenticated Key Exchange", <http://cat.inist.fr/?aModel=afficheN&cpsidt=14934236>, Jun. 24, 2004, pp. 1-44.

OCC Bulletin "Authentication in an Internet Banking Environment", http://www.ffiec.gov/pdf/authentication_guidance.pdf, pp. 2005, 1-16.

"FFIEC Releases Guidance on Authentication in Internet Banking Environment" <http://www.ffiec.gov/press/pr101205.htm>, Oct. 12, 2005.

* cited by examiner

Primary Examiner — William Goodchild

APPL-1003, ¶¶49-50.

Discussion Roadmap

- Ground 1:
 - POSITA would have combined Stone, Hoyos, and Varghese (Slides 9-24)
 - Limitations [1.2] and [1.9] (slides 26-31)
 - Claims 5, 8, 14, and 17 (slides 33-37)
- Ground 2: (slides 39-45)
 - POSITA would have combined Stone and Guidance.
- Grounds 3 and 4: (slides 47-50)
 - POSITA would have combined Stone-Hoyos-Varghese and Stone-Guidance with Borovsky

Claims 2, 3, 11, and 12

[2.0] The system of claim 1 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.

[3.0] The system of claim 2 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.

[11.0] The method of claim 10 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.

[12.0] The method of claim 11 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.

Prior Art: Borovsky

- Undisputed that Borovsky renders obvious the limitations of claims 2, 3, 11, and 12.
[2.0/11.0] The system of claim 1/method of claim 10 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.

[3.0/12.0] The system of claim 2/method of claim 11 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.
- The only disputed issue is motivation to combine Stone and Borovsky.

*“obtain the virtual likeness of
the face” of contacts
“from a social networking site”*

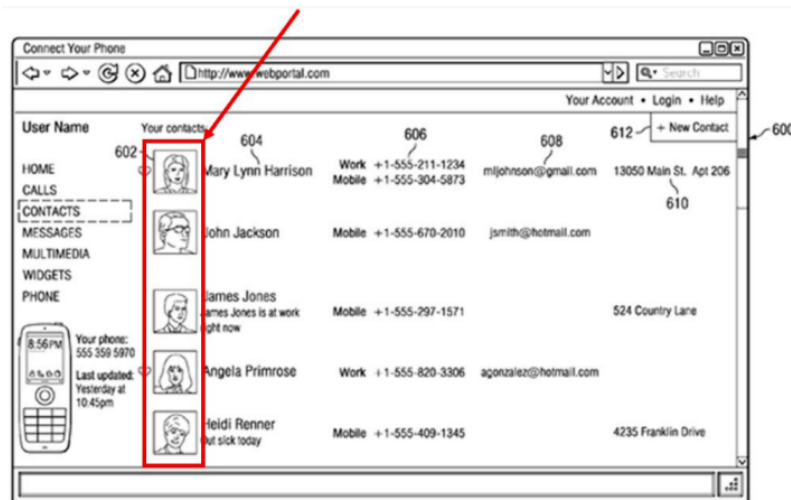


FIG. 6

(Borovsky) APPL-1041, FIG. 6; Pet. 77.

7. The system of claim 6, wherein:
the contacts interface enables the user to enter the contact management information by selecting one or more email accounts, social networking accounts, or instant messaging accounts of the user, wherein the third party servers comprise one or more email, social networking, or instant messaging servers corresponding to the one or more email, social networking, or instant messaging accounts, and wherein the third party information comprises contact information including one or more of:
names corresponding to contacts of the user, display names corresponding to contacts of the user, email addresses corresponding to contacts of the user, one phone numbers corresponding to contacts of the user, residential and other addresses corresponding to contacts of the user, photos corresponding to contacts of the user, and statuses corresponding to contacts of the user; and

(Borovsky) APPL-1041, claim 7; Pet. 76.

Grounds 3 and 4: POSITA Would Have Combined Stone and Borovsky

- **Stone has the need to obtain for display pictures of other network connected users.** Pet., 78; APPL-1003, ¶278 (citing APPL-1008, [0020], [0036]).
- **Borovsky’s known techniques would improve the user interface and user experience in Stone, in the same way when used according to Borovsky’s teachings.** Reply, 78.
- **POSITA would have reasonably expected to succeed in the combination.** Reply, 78..

the recipient”). Facing the need of displaying icons for other network connected users, a POSITA would have been motivated apply Borovsky’s teaching of providing user contact photo obtained from social network sites for display as icons for network-connected users, especially in the case that the other user did not profile a profile photo, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence (e.g., providing reassurance by seeing a recognizable photo), and efficient identification (e.g., easier identification of a recipient, esp. with common names). It was well-known that in mobile devices, profile images “can be created using a digital camera function of mobile device 504 or downloaded from various servers over a communications network,” including e.g., synchronize user device contact information including contact images using images from social network servers. *See e.g.,* (Chatterjee) APPL-1009,15:20-25; (Ekler) APPL-1042, 1.

“There is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’”

Intel Corp. v. PACT XPP Schweiz AG, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023).

Reply, 28.

PO's No-Combination Arguments are Misplaced.

PO's no-combination arguments are contrary to the law, contrary to the record, and disregard Petitioner's reasons to combine. Reply, 28.

- ✗ “Stone does not discuss using social networks to populate any information for the disclosed interface.”
- ✗ “Nothing in Stone suggests introducing another third-party server to Stone's existing client-server.”
- ✗ “The only motivation for doing would be conceived in hindsight.”

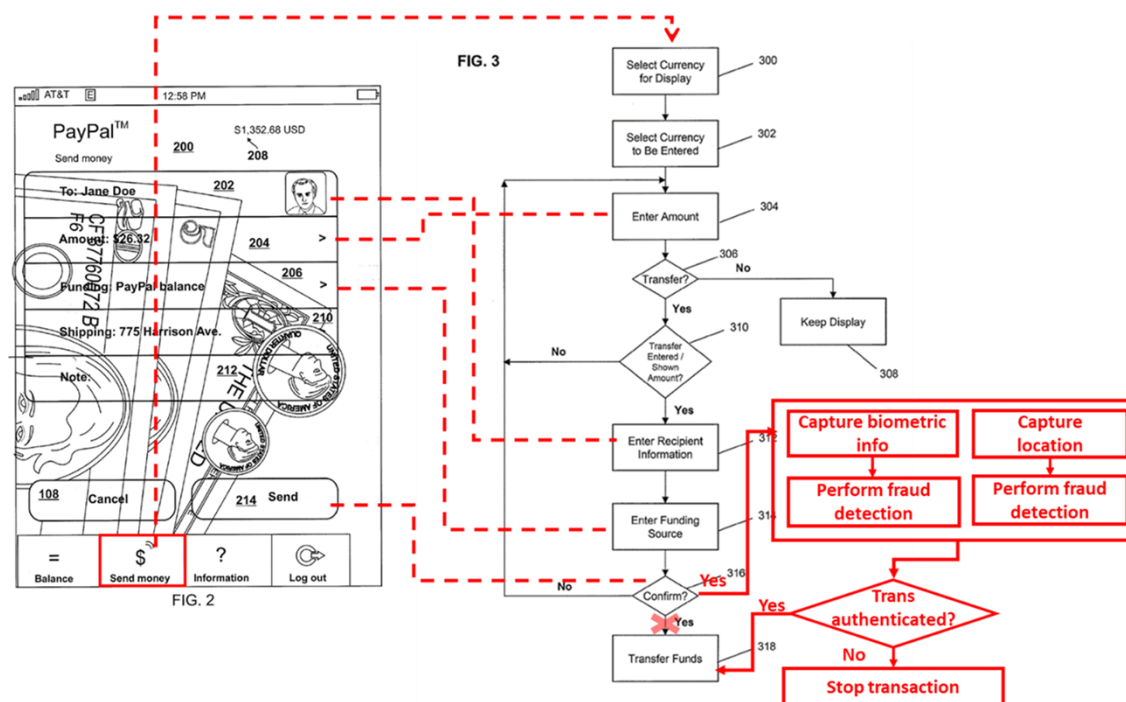
POR, 49.

THANK YOU. QUESTIONS?

BACKUP SLIDES

Undisputed that [1.6] is Rendered Obvious by Each of Grounds 1 and 2

[1.6] subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;



Example of Stone-Hoyos-Varghese

(annotated based on APPL-1008, FIGS. 2 and 3)

(Stone) APPL-1008, FIGS. 2 and 3; Pet. 46

To the Extent that it is Argued that “a Processor” Requires a Single Processor, Same Processor of User Device Renders Obvious the Processor of [1.2] And [1.9].

[1.2] **a processor configured to...** store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;

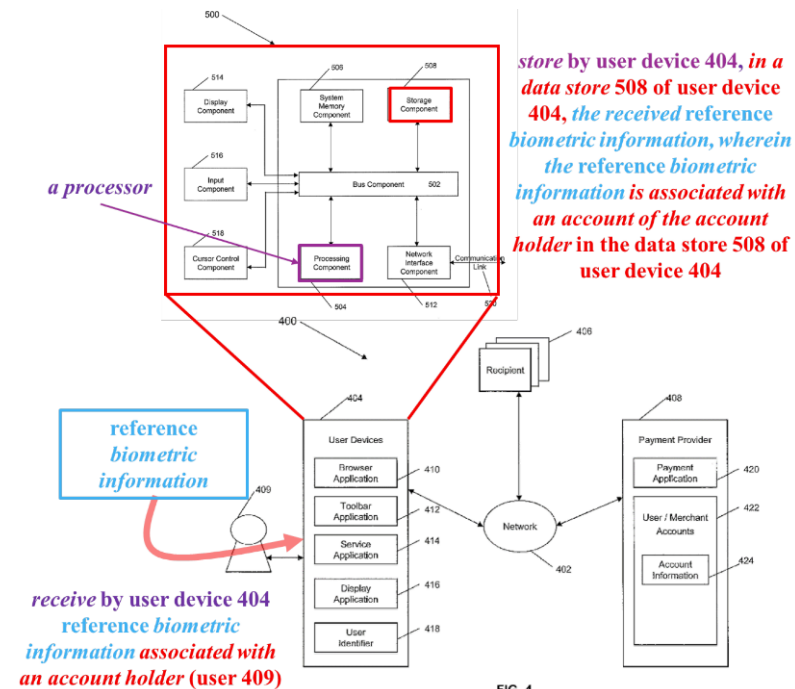


FIG. 4

Example of Stone Combined with Hoyos and Varghese (annotated based on APPL-1008, Stone, FIGS. 4 and 5).

Reply, 14.

[1.9] **a memory coupled to the processor and configured to provide the processor with instructions.**

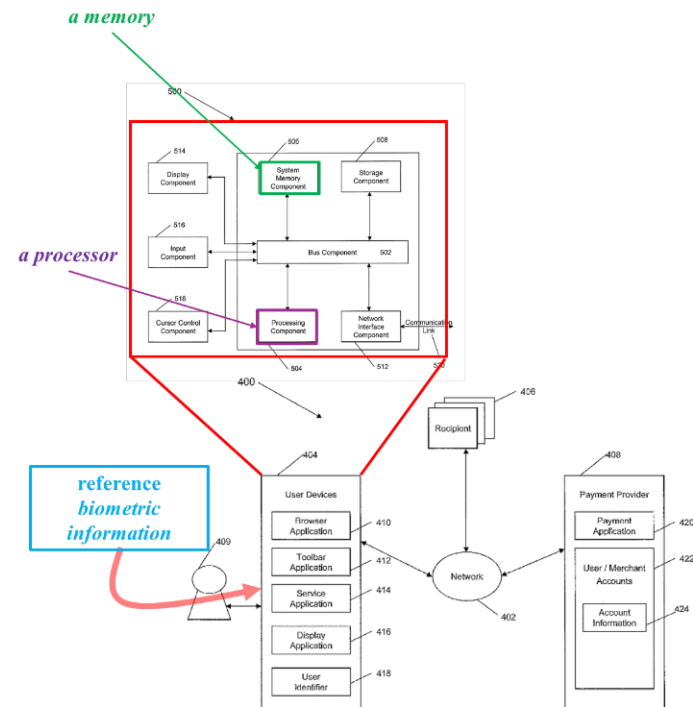


FIG. 4

Example of Stone Combined with Hoyos and Varghese (annotated based on APPL-1008, Stone, FIGS. 4 and 5).

Reply, 21.

Stored Biometric ID during Enrollment is Used For Subsequent Comparison With Later Captured Data for Authentication

Undisputed: Biometric information received during enrollment is used as the reference biometric information for authentication.

94. **Third**, to the extent that Patent Owner argues that Stone’s “biometric id” does not explicitly describe its use as the reference biometric information for comparison in biometric authentication, Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data.

(Hoyos) APPL-1013, [0003] (“Biometric identification and authentication systems are known in the art, for example systems to compare facial features, iris imagery, fingerprints, finger vein images, and palm vein images have been used. Such systems are known to be useful for [] comparing biometric data acquired from an individual to stored sets of biometric data of known “enrolled” individuals”). As discussed at VII.B.2, a POSITA would have been motivated to apply Hoyos’ fraud-resistant biometric authentication system in Stone, including implementing Hoyos’ teaching of capture and store enrollment biometric data during enrollment for subsequent comparison.

[0003] Biometric identification and authentication systems are known in the art, for example systems to compare facial features, iris imagery, fingerprints, finger vein images, and palm vein images have been used. Such systems are known to be useful for either comparing biometric data acquired from an individual to stored sets of biometric data of known “enrolled” individuals, or to compare biometric data acquired from an individual to a proposed template such as when an identification card is supplied to the system by the individual.

(Hoyos) APPL-1013, [0003]; Pet. 52.

(Jones Decl.) APPL-1003, 94; Pet. 51

Undisputed that Biometric Information Associated with a User Account is Fundamental Knowledge of Biometric Authentication.

[0009] A biometrics process using facial recognition will be described. First, a user must register user information in a biometrics system. For registration, the user has to input an image of his/her face via a device such as a camera for facial recognition. The input bio-information is raw data, and if this information is processed by a signal processing algorithm such as an image processor, feature data representing an individual's face can be obtained. This feature data functions as a standard template, and if the standard template is stored in a storage medium, the user's information registration process is completed. The type of the storage medium may be different according to the system used. In

(Lee) APPL-1014, [0009]; Pet. 32.

Enrollment Phase

In the enrollment phase 310, biometric data are acquired of physical features of a user. For example, the biometric data are derived from an image of a face, a recording of speech, an image of a fingerprint, or a scan of an iris.

Hereinafter, biometric data refers to the raw biometric signal sensed, measured or otherwise acquired from the physical features of the user. Features are extracted from the biometric data. The features are arranged in a d-dimensional feature vector. The feature vector forms enrollment biometric parameters 301. Methods for extracting features from various forms of biometric data are well known in the art, as described above. Conversion of the feature vector to biometric parameters and an optimal syndrome code are described in greater detail below.

(Draper) APPL-1023, 8:3-17; Pet. 32.

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis. Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

(FFIEC GUIDANCE) APPL-1037, 9-10; Pet. 32.

To the Extent that it is Argued That “a Processor” Requires a Single Processor, Ground 1 also Renders Claim 1 Obvious.

87. **Second**, to the extent that Patent Owner argues that “*a processor*” requires a **single** processor (contradictory to its own definition of “processor”), Stone alone or Stone-Hoyos-Varghese renders it obvious.

88. Specifically, as discussed at VII.B.2 and VII.B.3, a POSITA would have been motivated to implement various steps for an electronic transaction (e.g., steps of [1.2]-[1.8] discussed below) **locally** (e.g., on the user device of Stone) or remotely (e.g., on the service provider of Stone). For example, a POSITA would have been motivated to implement the authentication steps locally for the benefits including reduced latency, offline analysis capabilities, enhanced privacy, efficient resource utilization, customization for device characteristics, improved security.

See, e.g., (Mardikar) APPL-1015, (Carter) APPL-1016); APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042], [0076]. As such, to the extent that Patent Owner argues that “*a processor*” requires a **single** processor, Stone alone or Stone-Hoyos-Varghese renders obvious using a single processor of the user device to perform the processes discussed at [1.2]-[1.8] below.

PO does not dispute limitation [1.1], which recites: “a processor configured to:”

- **Dr. Jones explains that it would have been obvious to implement [1.2]-[1.8] locally.**
- **Undisputed benefits client-side local implementation.**

(Jones Decl.) APPL-1003, ¶¶ 87-88.

PO Mischaracterizes Stone as Requiring User Account Association to be Performed Only on Payment Server

27. PO appears to argue that because the payment server 408 maintains

the user accounts 422, the association of the reference biometric information with a

user account **has to** be performed by the payment server 408. This is incorrect. In

the system of Stone combined with Hoyos and Varghese where the biometric

authentication is performed locally on the user device, the reference biometric

information is stored **locally** and is associated with a user account for comparison

later on, which provides enhanced privacy and improved security. Pet. 20-21;

APPL-1003, ¶68 (citing APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042],

[0076], APPL-1038, 64); APPL-1016, [0040], [0042], [0076]; APPL-1038, 64

(“Biometric authentication can be implemented through systems performing the

matching either on the server or on the client side,” where describing “security and

privacy problems” and CPU-intensiveness of server side implementation, and

“relatively simple and cheap” with security and privacy benefits of client side

implementation).

Jones Supp. Decl., APPL-1056, ¶ 27.

END