CARBYNE BIOMETRICS, LLC

Oral Argument for

IPR2024-00329 (U.S. PATENT NO. 9,972,010),
IPR2024-00330 (U.S. PATENT NO. 10,713,656),
and
IPR2024-00331 (U.S. PATENT NO 11,526,886)

Before Administrative Patent Judges

- Jameson Lee
- Arthur Peslak
- Steven Amundson

McKool Smith

Table of Contents

Fraud Reduction Patents and Petitioner's References

'010 Patent & Universal Arguments

- No Motivation to Combine Stone and Hoyos.
- No Motivation to Combine Stone and FFIEC Guidance.
- Limitations [1.2]-[1.5]: Stone-Hoyos does not disclose or render obvious the "virtual likeness of the face of the account holder."
- Stone-Hoyos does not disclose "memory" limitations.

'656 Patent

- Limitation [1.2]: Stone-Hoyos-Varghese does not disclose or render obvious "store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder."

'886 Patent

- Limitation [1.2.2]: Stone-Hoyos-Varghese does not render obvious "wherein the virtual likeness of the face was selected by the account holder as part of an enrollment."
- Limitation [1.3.1]: Stone-Hoyos-Varghese does not disclose or render obvious "subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capture contextual information comprising location data."

The Fraud Reduction Patents

’010 Patent

US009972010B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 9,972,010 B1**
(45) **Date of Patent: *May 15, 2018**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days. days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/875,245**

(22) Filed: **May 1, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/4014*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 30/06; G06Q 30/0633; G06Q 30/0601; G06Q 30/0641; G06Q 20/4014
USPC 705/26.1, 27.1, 26.81
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A *	6/1995	Haynes	G06F 3/0486 715/769
6,091,835	A *	7/2000	Smithies	G06K 9/00154 340/5.86
6,208,659	B1 *	3/2001	Govindarajan	G06Q 30/06 370/400
6,851,094	B1 *	2/2005	Robertson	G06F 17/5045 709/217
7,930,220	B1 *	4/2011	Gaw	G06Q 30/0601 705/26.1
2001/0042042	A1 *	11/2001	Stokes	G06Q 20/04 705/42
2002/0046055	A1 *	4/2002	Martino	G06Q 20/341 705/50
2002/0116293	A1 *	8/2002	Lao	G06F 17/3080 705/27.1
2002/0152137	A1 *	10/2002	Lindquist	G06Q 30/06 705/26.8

(Continued)

OTHER PUBLICATIONS

Art Explosion, Nova Development 2002.*

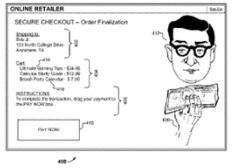
(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets



APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00329, APPL-1001

’656 Patent

US010713656B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 10,713,656 B1**
(45) **Date of Patent: *Jul. 14, 2020**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **RightQuestion, LLC**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 274 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/948,744**

(22) Filed: **Apr. 9, 2018**

Related U.S. Application Data

(63) Continuation of application No. 13/875,245, filed on May 1, 2013, now Pat. No. 9,972,010, which is a continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/06 (2012.01)

(52) **U.S. Cl.**
CPC ... ***G06Q 20/4014*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 30/06*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4014; G06Q 20/40145; G06Q 20/4016; G06Q 30/06; G06Q 30/0601; G06Q 30/0643
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A	6/1995	Haynes	
6,091,835	A	7/2000	Smithies	
6,208,659	B1	3/2001	Govindarajan	
6,851,094	B1	2/2005	Robertson	
7,930,220	B1	4/2011	Gaw	
2001/0026632	A1 *	10/2001	Tamai	G06K 9/00597 382/116
2001/0042042	A1	11/2001	Stokes	
2002/0046055	A1	4/2002	Martino	
2002/0116293	A1	8/2002	Lao	

(Continued)

OTHER PUBLICATIONS

Boukhonine, Sergasi, Vlad Krotov, and Barry Rupert. "Future security approaches and biometrics." Communications of the Association for Information Systems 16.1 (2005): 48. (Year: 2005).*

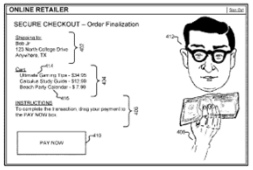
(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

19 Claims, 12 Drawing Sheets



APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00330, APPL-1001

’886 Patent

US011526886B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 11,526,886 B1**
(45) **Date of Patent: *Dec. 13, 2022**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **RightQuestion, LLC**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/893,237**

(22) Filed: **Jun. 4, 2020**

Related U.S. Application Data

(63) Continuation of application No. 15/948,744, filed on Apr. 9, 2018, now Pat. No. 10,713,656, which is a continuation of application No. 13/875,245, filed on May 1, 2013, now Pat. No. 9,972,010, which is a continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/06 (2012.01)

(52) **U.S. Cl.**
CPC ... ***G06Q 20/4014*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 30/06*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4014; G06Q 20/40145; G06Q 30/06; G06Q 30/0641-0643
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A	6/1995	Haynes
6,091,835	A	7/2000	Smithies
6,208,659	B1	3/2001	Govindarajan
6,851,094	B1	2/2005	Robertson
7,930,220	B1	4/2011	Gaw
2001/0026632	A1	10/2001	Tamai
2001/0042042	A1	11/2001	Stokes
2002/0046055	A1	4/2002	Martino
2002/0116293	A1	8/2002	Lao

(Continued)

OTHER PUBLICATIONS

Reddy, P. Venkata, et al. "A new antispoofing approach for biometric devices." IEEE transactions on biomedical circuits and systems 2.4 (2008): 328-337. (Year: 2008).*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets

APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00331, APPL-1001

The Fraud Reduction Patents

User Interface

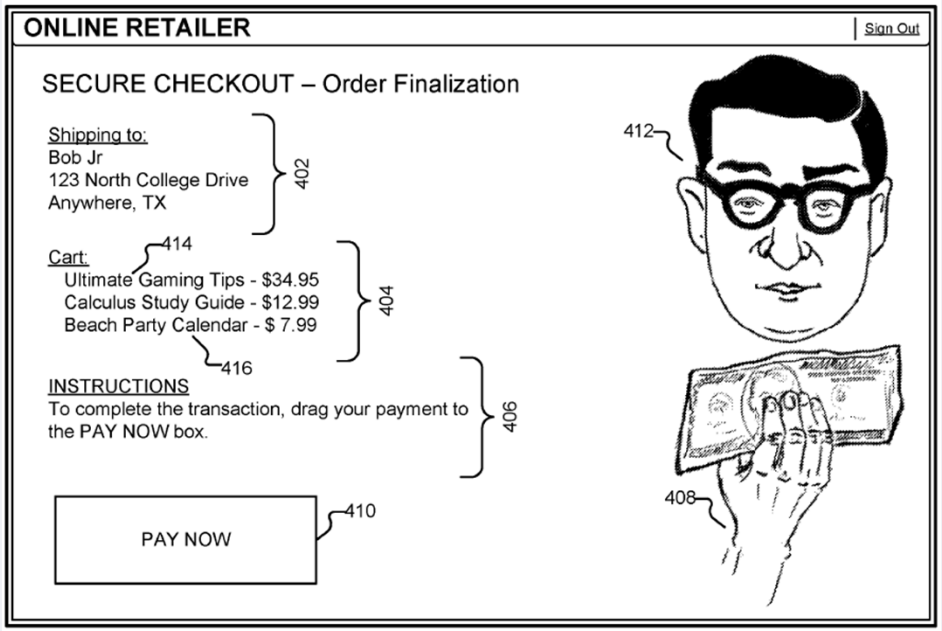


FIG. 4

APPL-1001, Fig. 4

Fraud Detection

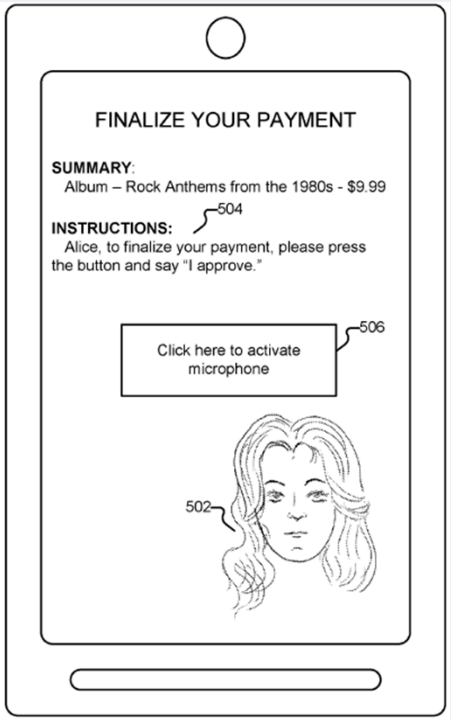


FIG. 6

APPL-1001, Fig. 6

POR [17] at 1-6 **All citations are to the '010 Patent unless stated otherwise.*

Representative Claims

’010 Patent

1. A system, comprising:
one or more processors configured to:
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;
render, in an interface, the virtual likeness of the face of the account holder;
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;
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;
capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
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
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
a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

IPR2023-00329, APPL-1001, ’010 Patent Cl. 1

’656 Patent

1. A system, comprising:
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;
render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
render, in the one or more interfaces, a transaction icon associated with the electronic transaction;
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;
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;
perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
determining, based at least in part on the captured biometric information, that the user is alive; and
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
a memory coupled to the processor and configured to provide the processor with instructions.

IPR2023-00330, APPL-1001, ’656 Patent Cl. 1

’886 Patent

1. A system, comprising:
one or more processors configured to:
render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
capture contextual information comprising location data usable to determine a physical location associated with the user; and
capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
the physical location associated with the user determined using the captured location data; and
an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and
a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

Interface Limitations

’010 Patent

1. A system, comprising:
one or more processors configured to:
receive a virtual likeness of a face of an account holder;
associate, in a data store, the virtual likeness of the face

render, in an interface, the virtual likeness of the face of the account holder;
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;
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;

capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
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
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
a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

IPR2023-00329, APPL-1001, ’010 Patent Cl. 1

’656 Patent

1. A system, comprising:
a processor configured to:
receive biometric information associated with an account holder;

render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
render, in the one or more interfaces, a transaction icon associated with the electronic transaction;
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;

action icon rendered in the one or more interfaces;
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;
perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
determining, based at least in part on the captured biometric information, that the user is alive; and
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
a memory coupled to the processor and configured to provide the processor with instructions.

IPR2023-00330, APPL-1001, ’656 Patent Cl. 1

’886 Patent

1. A system, comprising:
one or more processors configured to:

render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;

subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
capture contextual information comprising location data usable to determine a physical location associated with the user; and
capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
the physical location associated with the user determined using the captured location data; and
an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and
a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

Fraud Detection Limitations

’010 Patent

1. A system, comprising:
one or more processors configured to:
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;
render, in an interface, the virtual likeness of the face of the account holder;
render a transaction icon associated with an electronic

capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
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

analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
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
a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

IPR2023-00329, APPL-1001, ’010 Patent Cl. 1

’656 Patent

1. A system, comprising:
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;
render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;

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;
perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
determining, based at least in part on the captured biometric information, that the user is alive; and

determining, based at least in part on the captured biometric information, that the user is alive; and
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
a memory coupled to the processor and configured to provide the processor with instructions.

IPR2023-00330, APPL-1001, ’656 Patent Cl. 1

’886 Patent

1. A system, comprising:
one or more processors configured to:
render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;

subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
capture contextual information comprising location data usable to determine a physical location associated with the user; and
capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
the physical location associated with the user determined using the captured location data; and
an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and

a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

Petitioner's Grounds

IPR2023-00329 ('010 Patent)

- Ground 1: Stone combined with Hoyos
- Ground 2: Stone in view of Hoyos and Varghese
- Ground 3: Stone combined with FFIEC Guidance

IPR2023-00330 ('656 Patent)

- Ground 1: Combination of Stone, Hoyos, and Varghese
- Ground 2: Stone combined with FFIEC Guidance
- Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Borovsky (Ground 3) and combination of Stone, FFIEC Guidance, and Borovsky (Ground 4)

IPR2023-00331 ('886 Patent)

- Ground 1: Stone combined with Hoyos and Varghese
- Ground 2: Stone combined with FFIEC Guidance
- Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Campbell (Ground 3) and combination of Stone, FFIEC Guidance, and Campbell (Ground 4)

See generally POR; Sur-Reply

"Stone" US 2010/0042535 A1

US 20100042535A1

(19) United States
(12) Patent Application Publication
Stone
(10) Pub. No.: US 2010/0042535 A1
(43) Pub. Date: Feb. 18, 2010

(54) CURRENCY DISPLAY

(75) Inventor: Carl B. Stone, Campbell, CA (US)

Correspondence Address:
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, SUITE 700
Dallas, TX 75219 (US)

(73) Assignee: eBay Inc., San Jose, CA (US)

(21) Appl. No.: 12/192,479

(22) Filed: Aug. 15, 2008

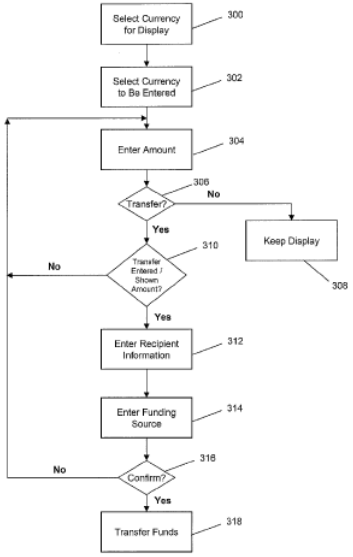
Publication Classification

(51) Int. Cl.
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) U.S. Cl. 705/39; 705/1

(57) ABSTRACT

Actual currency is shown displayed on a user device, where the currency represents an amount of money selected by the user. For example, if the user selects $86.21 for U.S. Dollars, the display will show four twenty dollar bills, one five dollar bill, one one dollar bill, two dimes, and one penny.



APPL-1008
APPLE INC. / Page 1 of 12

CURRENCY DISPLAY

BACKGROUND

[0001] 1. Field of Invention

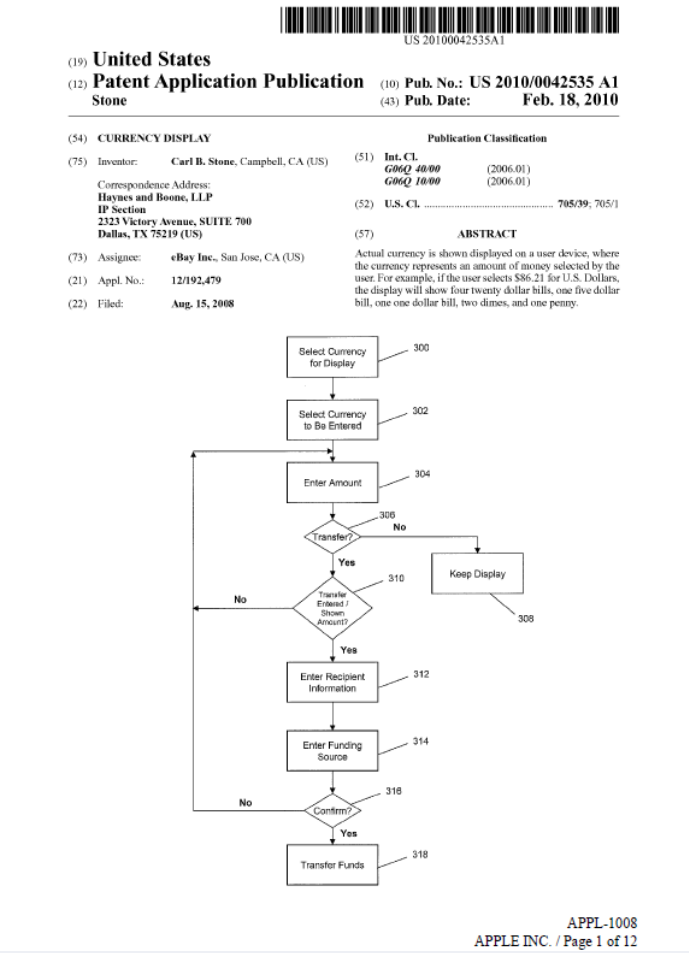
[0002] The present invention relates to electronic visual displays, and in particular, to such displays that show a visual representation of financial instruments.

DETAILED DESCRIPTION

[0016] Embodiments of the present disclosure enable users to see a selected actual currency representing the amount entered by the user into a device with a display screen. For example, if the user enters $33.26 in U.S. dollars, the display will show one U.S. twenty dollar bill, one U.S. ten dollar bill, three U.S. one dollar bills, one U.S. quarter, and one U.S. penny. This gives the user a visual representation of the amount, which reinforces the value of the amount and provides the user with a more visually rich interface.

See Ex. 1008 (Stone)

"Stone" US 2010/0042535 A1



US 20100042535A1

(19) **United States**

(12) **Patent Application Publication**

Stone

(10) **Pub. No.: US 2010/0042535 A1**

(43) **Pub. Date: Feb. 18, 2010**

(54) **CURRENCY DISPLAY**

(75) Inventor: **Carl B. Stone**, Campbell, CA (US)

Correspondence Address:
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, SUITE 700
Dallas, TX 75219 (US)

(73) Assignee: **eBay Inc.**, San Jose, CA (US)

(21) Appl. No.: **12/192,479**

(22) Filed: **Aug. 15, 2008**

Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) **U.S. Cl.** **705/39**; 705/1

(57) **ABSTRACT**

Actual currency is shown displayed on a user device, where the currency represents an amount of money selected by the user. For example, if the user selects $86.21 for U.S. Dollars, the display will show four twenty dollar bills, one five dollar bill, one one dollar bill, two dimes, and one penny.

APPL-1008
APPLE INC. / Page 1 of 12

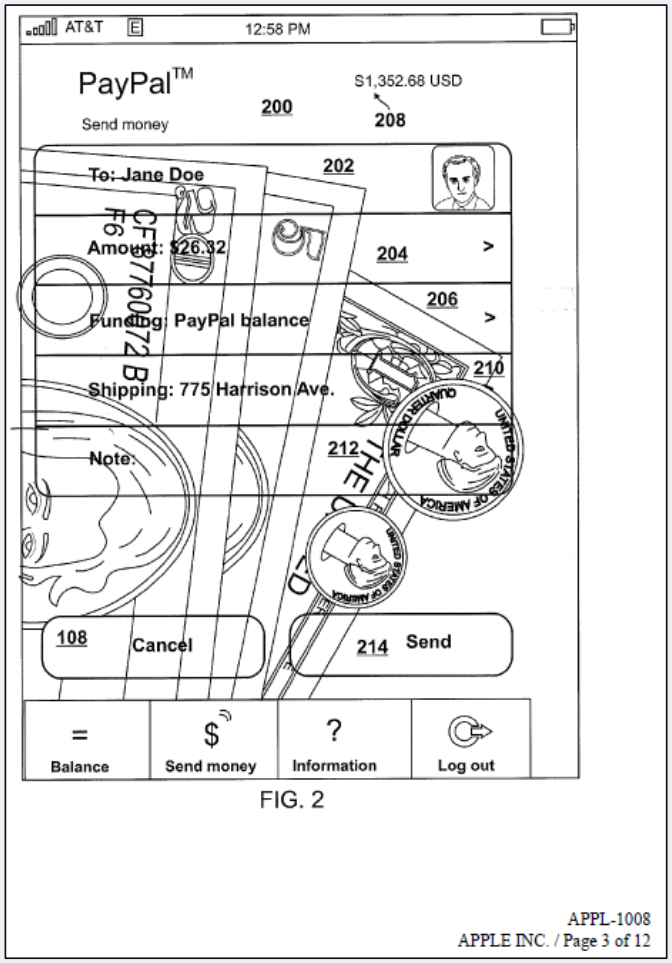
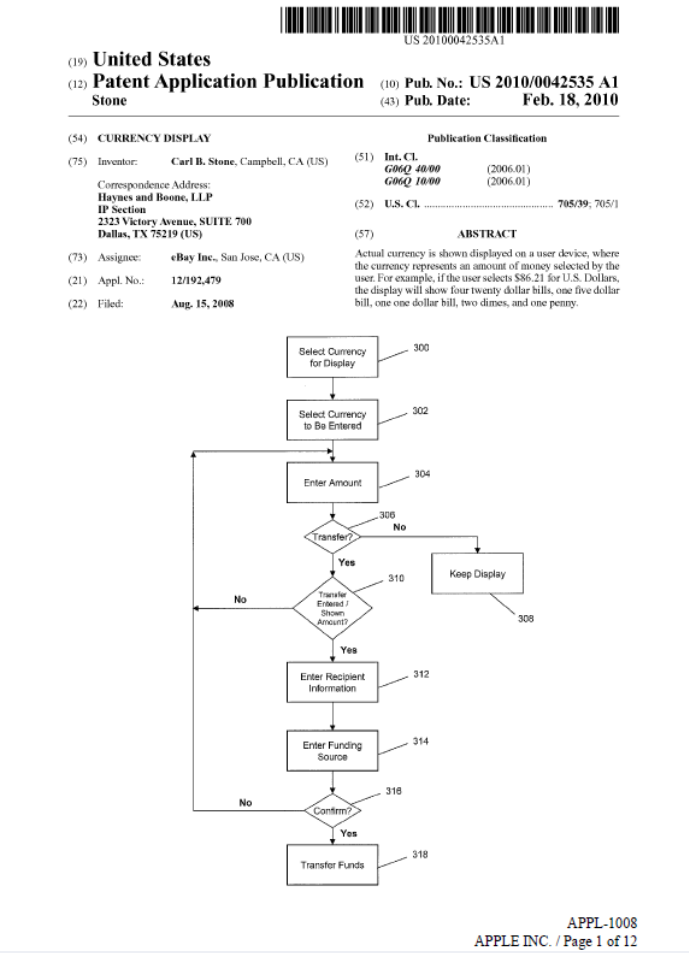


FIG. 2

APPL-1008
APPLE INC. / Page 3 of 12

See Ex. 1008 (Stone)

"Stone" US 2010/0042535 A1



US 20100042535A1

(19) **United States**

(12) **Patent Application Publication**

Stone

(10) **Pub. No.: US 2010/0042535 A1**

(43) **Pub. Date: Feb. 18, 2010**

(54) **CURRENCY DISPLAY**

(75) Inventor: **Carl B. Stone**, Campbell, CA (US)

Correspondence Address:
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, SUITE 700
Dallas, TX 75219 (US)

(73) Assignee: **eBay Inc.**, San Jose, CA (US)

(21) Appl. No.: **12/192,479**

(22) Filed: **Aug. 15, 2008**

Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) **U.S. Cl.** **705/39**; 705/1

(57) **ABSTRACT**

Actual currency is shown displayed on a user device, where the currency represents an amount of money selected by the user. For example, if the user selects $86.21 for U.S. Dollars, the display will show four twenty dollar bills, one five dollar bill, one one dollar bill, two dimes, and one penny.

APPL-1008
APPLE INC. / Page 1 of 12

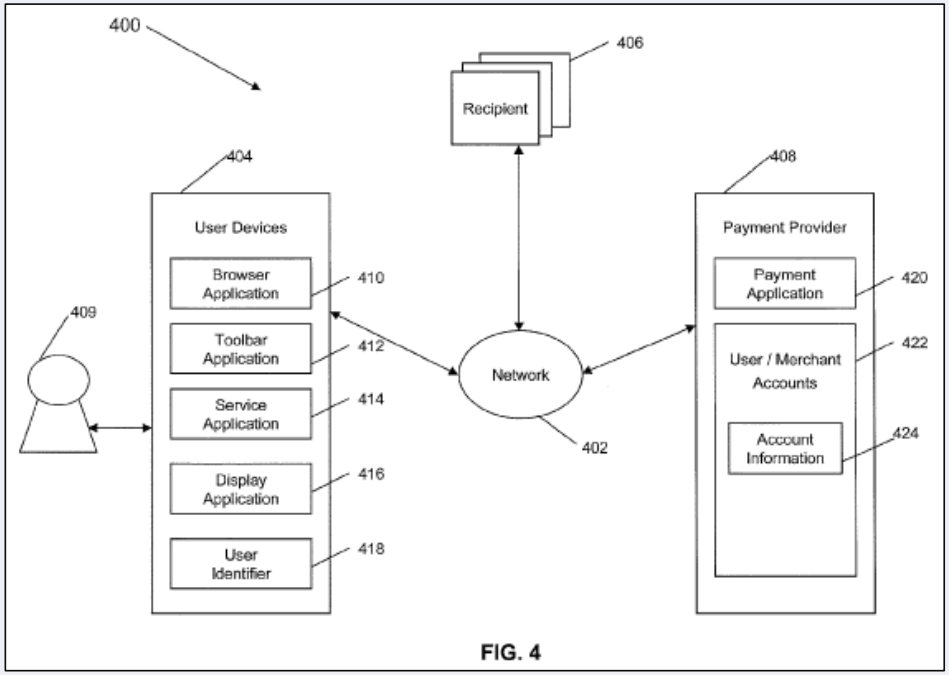
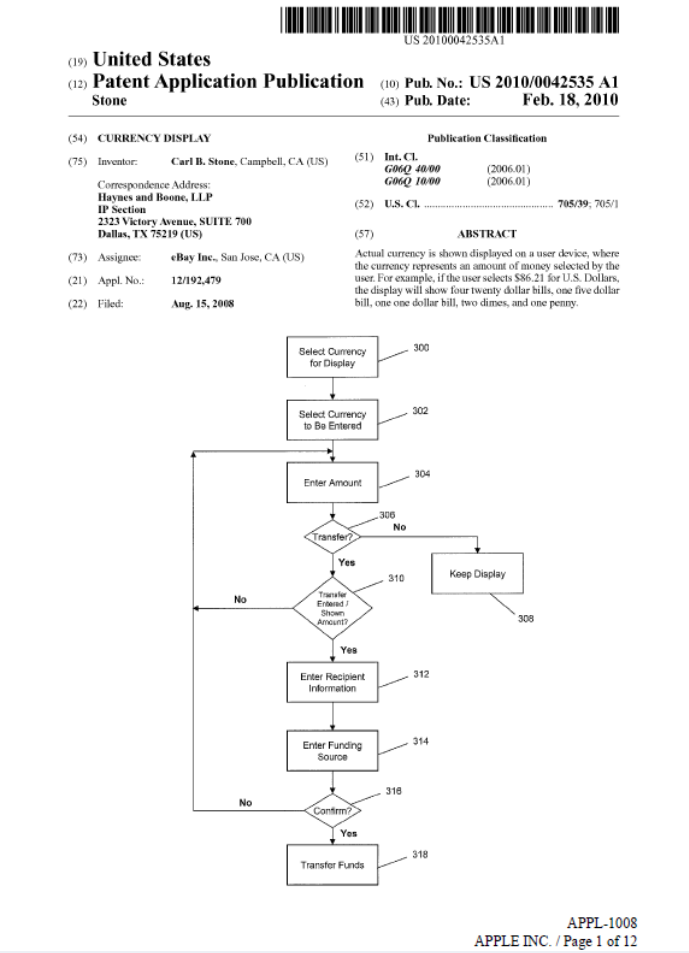


FIG. 4

See Ex. 1008 (Stone)

“Stone” US 2010/0042535 A1



US 20100042535A1

(19) **United States**

(12) **Patent Application Publication**

Stone

(10) **Pub. No.: US 2010/0042535 A1**

(43) **Pub. Date: Feb. 18, 2010**

(54) **CURRENCY DISPLAY**

(75) Inventor: **Carl B. Stone**, Campbell, CA (US)

Correspondence Address:
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, SUITE 700
Dallas, TX 75219 (US)

(73) Assignee: **eBay Inc.**, San Jose, CA (US)

(21) Appl. No.: **12/192,479**

(22) Filed: **Aug. 15, 2008**

Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) **U.S. Cl.** **705/39**; 705/1

(57) **ABSTRACT**

Actual currency is shown displayed on a user device, where the currency represents an amount of money selected by the user. For example, if the user selects $86.21 for U.S. Dollars, the display will show four twenty dollar bills, one five dollar bill, one one dollar bill, two dimes, and one penny.

APPL-1008
APPLE INC. / Page 1 of 12

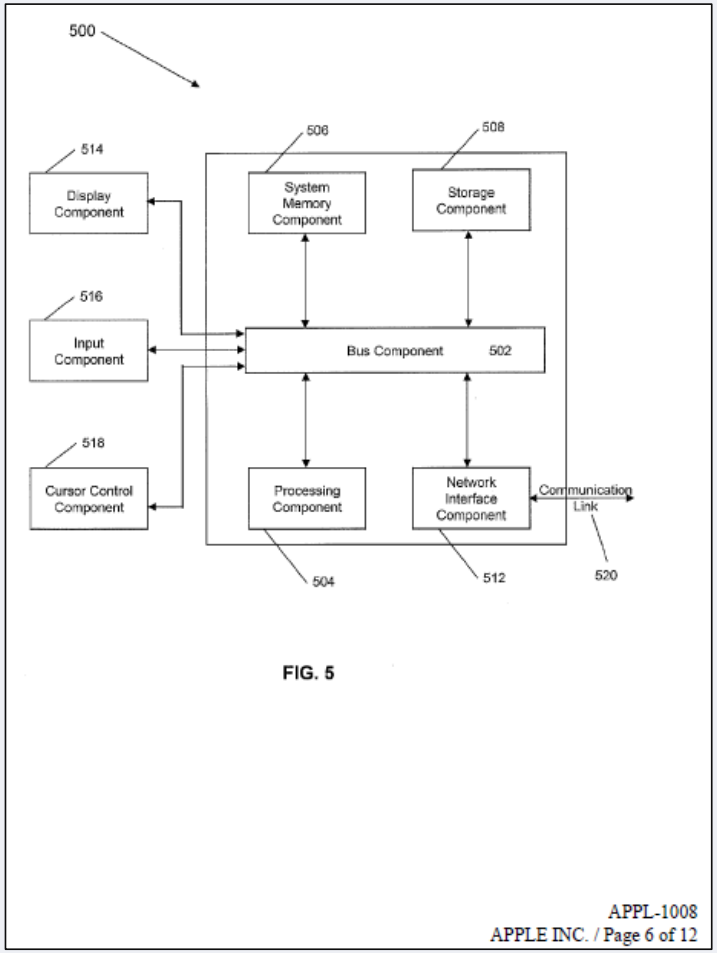


FIG. 5

APPL-1008
APPLE INC. / Page 6 of 12

See Ex. 1008 (Stone)

“Hoyos” US 2010/0014720 A1

US 20100014720A1

(19) United States
(12) Patent Application Publication
Hoyos et al.
(10) Pub. No.: US 2010/0014720 A1
(43) Pub. Date: Jan. 21, 2010

(54) FRAUD RESISTANT BIOMETRIC FINANCIAL TRANSACTION SYSTEM AND METHOD

(76) Inventors: Hector T. Hoyos, New York, NY (US); Keith J. Hanna, New York, NY (US)

Correspondence Address:
PRYOR CASHMAN, LLP
7 Times Square
NEW YORK, NY 10036-6569 (US)

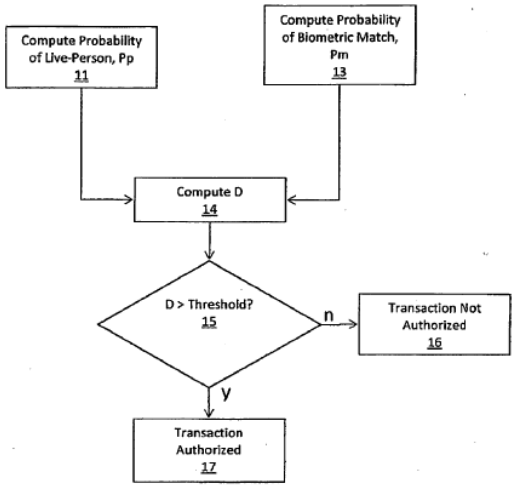
(21) Appl. No.: 12/444,018
(22) PCT Filed: Oct. 2, 2007
(86) PCT No.: PCT/US07/80135
§ 371 (c)(1), (2), (4) Date: Apr. 2, 2009

Related U.S. Application Data
(60) Provisional application No. 60/827,738, filed on Oct. 2, 2006.

Publication Classification
(51) Int. Cl. G06K 9/00 (2006.01)
(52) U.S. Cl. 382/118; 382/115; 382/124

(57) ABSTRACT

A method and system for authenticating financial transactions is disclosed wherein biometric data is acquired from a person and the probability of liveness of the person and probability of a match between the person or token and known biometric or token information are calculated, preferably according to a formula D=P(p)*(K+P(m)), wherein K is a number between 0.1 and 100, and authenticating if the value of D exceeds a predetermined value.



(57) ABSTRACT

A method and system for authenticating financial transactions is disclosed wherein biometric data is acquired from a person and the probability of liveness of the person and probability of a match between the person or token and known biometric or token information are calculated, preferably according to a formula D=P(p)*(K+P(m)), wherein K is a number between 0.1 and 100, and authenticating if the value of D exceeds a predetermined value.

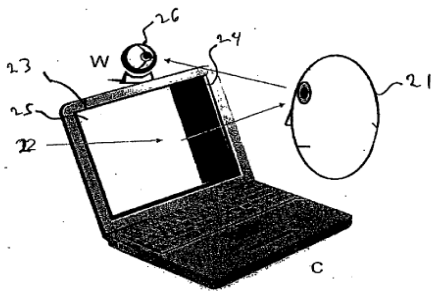
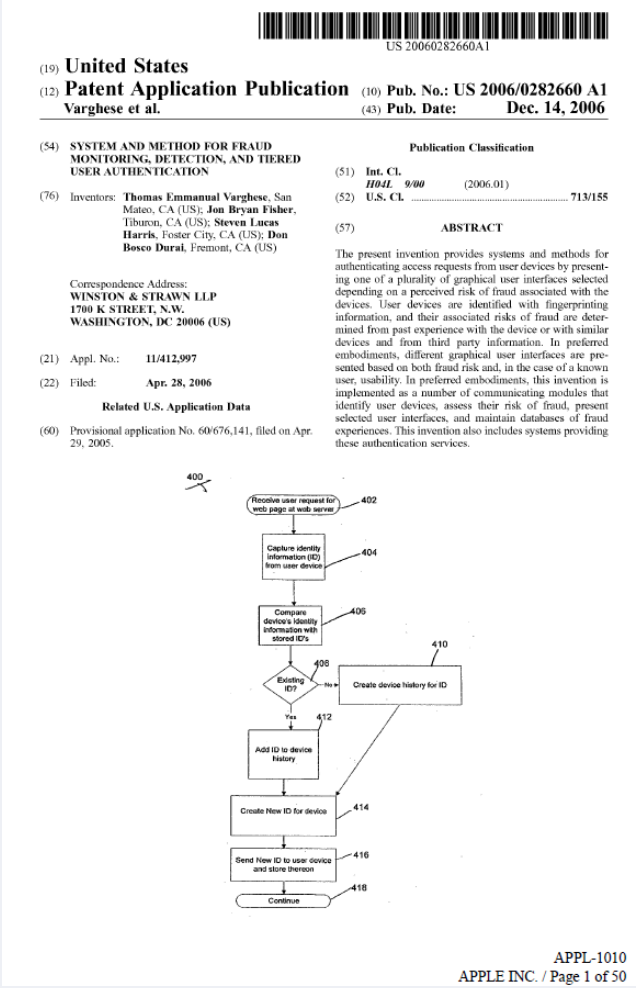


Fig. 2

See Ex. 1013 (Hoyos)

“Varghese” US 2006/0282660 A1



US 20060282660A1

(19) **United States**

(12) **Patent Application Publication**

Varghese et al.

(10) **Pub. No.: US 2006/0282660 A1**

(43) **Pub. Date: Dec. 14, 2006**

(54) **SYSTEM AND METHOD FOR FRAUD MONITORING, DETECTION, AND TIERED USER AUTHENTICATION**

(76) Inventors: **Thomas Emmanual Varghese**, San Mateo, CA (US); **Jon Bryan Fisher**, Tiburon, CA (US); **Steven Lucas Harris**, Foster City, CA (US); **Don Bosco Durai**, Fremont, CA (US)

Correspondence Address:
WINSTON & STRAWN LLP
1700 K STREET, N.W.
WASHINGTON, DC 20006 (US)

(21) Appl. No.: **11/412,997**

(22) Filed: **Apr. 28, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/676,141, filed on Apr. 29, 2005.

Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/155**

(57) **ABSTRACT**

The present invention provides systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices. User devices are identified with fingerprinting information, and their associated risks of fraud are determined from past experience with the device or with similar devices and from third party information. In preferred embodiments, different graphical user interfaces are presented based on both fraud risk and, in the case of a known user, usability. In preferred embodiments, this invention is implemented as a number of communicating modules that identify user devices, assess their risk of fraud, present selected user interfaces, and maintain databases of fraud experiences. This invention also includes systems providing these authentication services.

APPL-1010
APPLE INC. / Page 1 of 50

(57) **ABSTRACT**

The present invention provides systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices. User devices are identified with fingerprinting information, and their associated risks of fraud are determined from past experience with the device or with similar devices and from third party information. In preferred embodiments, different graphical user interfaces are presented based on both fraud risk and, in the case of a known user, usability. In preferred embodiments, this invention is implemented as a number of communicating modules that identify user devices, assess their risk of fraud, present selected user interfaces, and maintain databases of fraud experiences. This invention also includes systems providing these authentication services.

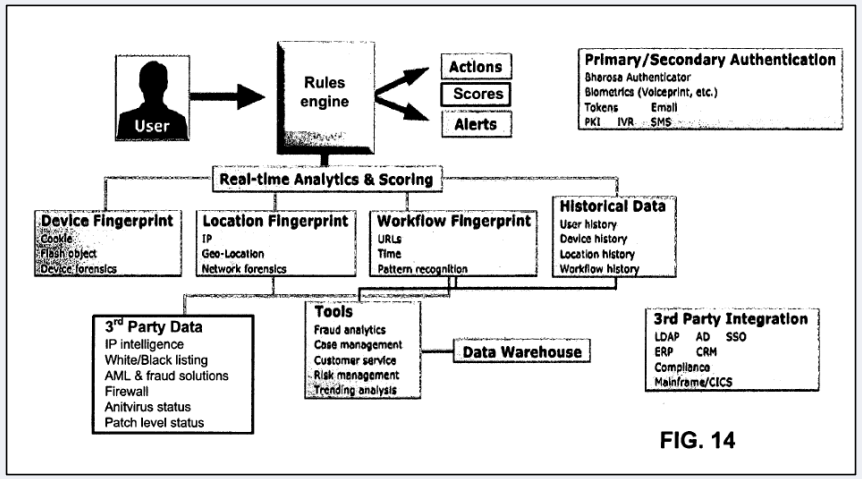


FIG. 14

See Ex. 1010 (Varghese)

"FFIEC Guidance" – Authentication in an Internet Banking Environment

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (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.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, 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. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.
[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

APPL-1037
APPLE INC./Page 1 of 14

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;
- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and
- Implement appropriate risk mitigation strategies.

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.
[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

See Ex. 1037 (FFIEC Guidance)

’010 Patent and Universal Arguments

No Motivation to Combine Stone and Hoyos

Petitioner's Alleged Motivation to Combine Stone and Hoyos

2. Combination of Stone and Hoyos ("Stone-Hoyos")

A POSITA would have been motivated to apply Hoyos' teaching of fraud resistant biometric financial transaction system in Stone's financial transactions, for the benefits of improved fraud resistancy by addressing spoofing and achieving "improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers" as taught by Hoyos. APPL-1013, [0015], [0017]-[0022]; APPL-1003, ¶¶59-68.

Petition [2] at 17

Petitioner's Alleged Motivation to Combine Stone and Hoyos

In view of Stone's need to implement authentication with fraud detection, a POSITA would have implemented biometric authentication and fraud detection as taught by Hoyos in the system of Stone. APPL-1003, ¶62. By authorizing transactions "by combining in one algorithm the live-person result with the match result," various advantages are achieved using Hoyos' biometric authentication method, including addressing spoofing; "making it much more difficult for an attempted fraudster to refine fraudulent methods" and thereby reducing iterative attacks by eliminating clear feedback; greatly reducing "the reject rate of true authentics" by using the liveness probability that is less sensitive to conditions like illumination changes; providing "an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them;" and by ensuring that some live-person data is captured, providing "a means to perform customer redress." APPL-1013, [0024],

Petition [2] at 18

No Motivation to Combine Stone-Hoyos

Petitioner's Alleged Motivation to Combine
Is Conclusory and Unsupported

> "[C]onclusory assertion[s] with no explanation [are] inadequate to support a finding that there would have been a motivation to combine."

TQ Delta, LLC v. CISCO Sys., Inc.,
942 F.3d 1352, 1356 (Fed. Cir. 2019).

POR [17] at 23

No Motivation to Combine Stone-Hoyos

- Petitioner presupposes the "problem" of electronic fraud *and*
- assumes a POSITA would apply a specific class of fraud detection techniques (anti-spoofing/aliveness) without explaining why a PO.

But as the POR explains, Petitioner's justification for combining Stone and Hoyos is conclusory. POR, 23-26; Ex. 2032 ¶¶ 66-70. It overgeneralizes and presupposes the problem of electronic fraud and assumes a POSITA would apply a narrow class of fraud detection techniques (aliveness detection) without explaining why a POSITA would choose these techniques over others. POR, 23-26. For one,

22

Sur-Reply [20] at 22

No Motivation to Combine Stone-Hoyos

Stone does not identify fraud as a problem or anti-spoofing as a solution.

IPR2024-00329
U.S. Patent No. 9,972,010

Petitioner has provided no evidence "that financial *transactions of Stone* had a need for authentication including fraud detection." Pet., 17 (emphasis added). Stone itself does not identify payment fraud as a problem that needs addressing. POR, 28, Ex. 2032 ¶ 76. The sources Petitioner cites identify a need for higher security authentication in high-risk banking and financial institution transactions over certain dollar amounts. *See* Pet., 17-18, citing Ex. 1010 (noting banks and financial institutions may want higher security authentication for transactions over a certain amount); Ex. 1016 (patent application assigned to Bank of America noting that

Sur-Reply [20] at 23

Stone Is Not Analogous Art

Test for Analogous Art

"Prior art is analogous where either (1) 'the art is from the same field of endeavor, regardless of the problem addressed' or (2) even if the reference is not within the same field of endeavor, 'the reference still is reasonably pertinent to the particular problem with which the inventor is involved.'"

In re Ethicon, Inc., 844 F.3d 1344, 1349 (Fed. Cir. 2017)
(quoting *In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992))

POR [17] at 26-27

Stone Is Not Analogous Art

The field of endeavor cannot be defined "too broadly."

"[T]he field of endeavor cannot be defined "too broadly" such that it would be beyond what a POSITA would reasonably be expected to look for to find a solution to the problem facing the inventor."

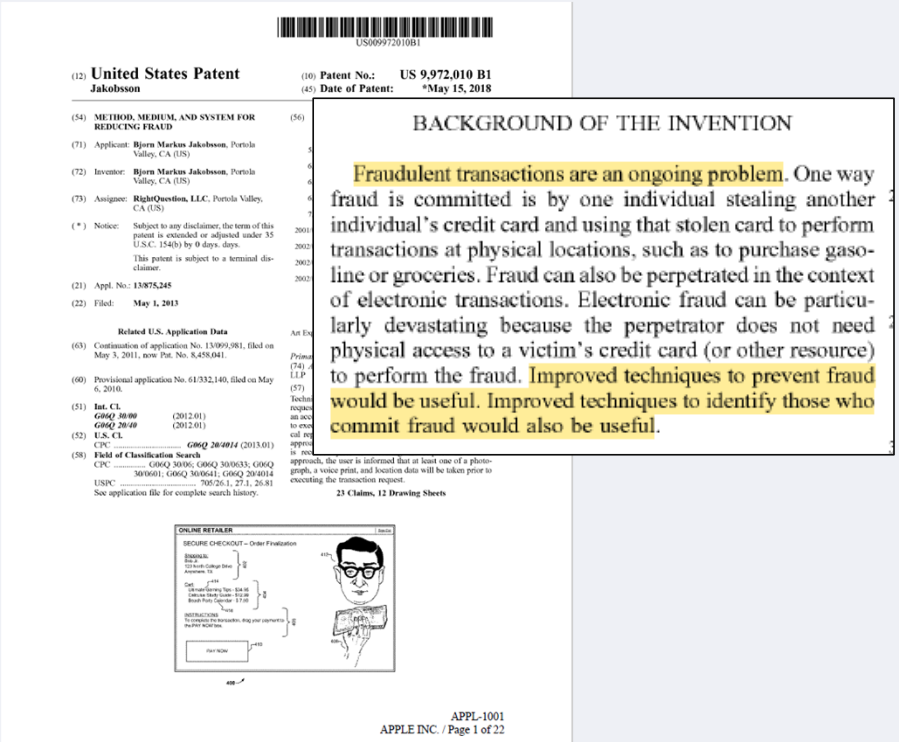
See Fresenius Med. Care Holdings, Inc. v. Baxter Int'l., Inc., No. C 03-1431 SBA, 2006 WL 1343648, at *22 (N.D. Cal. May 16, 2006)

POR [17] at 27

Stone Is Not Analogous Art

Not the same field of endeavor and not directed to the same problem.

’010 Patent



US009972010B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 9,972,010 B1**
(45) **Date of Patent: *May 15, 2018**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days. days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/875,245**

(22) Filed: **May 1, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/4014*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 30/06; G06Q 30/0633; G06Q 30/0601; G06Q 30/0641; G06Q 20/4014
USPC 705/26.1, 27.1, 26.81
See application file for complete search history.

23 Claims, 12 Drawing Sheets

ONLINE RETAILER

SECURE CHECKOUT – Order Finalization

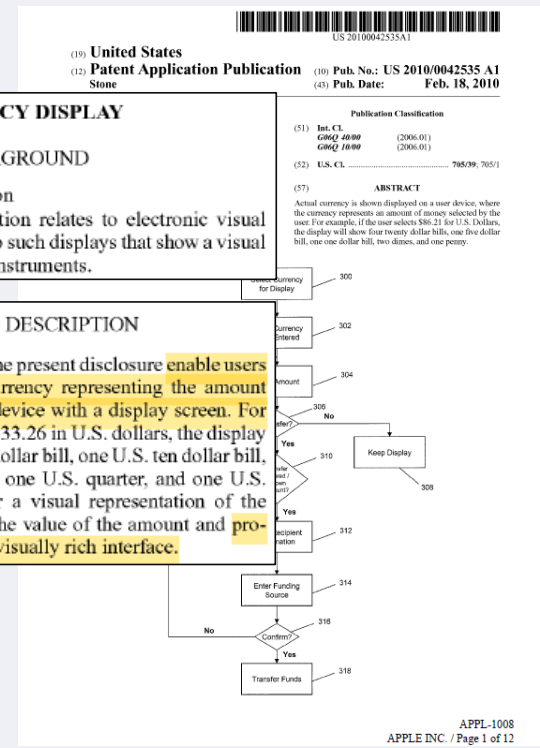
APPL-1001
APPLE INC. / Page 1 of 22

BACKGROUND OF THE INVENTION

Fraudulent transactions are an ongoing problem. One way fraud is committed is by one individual stealing another individual’s credit card and using that stolen card to perform transactions at physical locations, such as to purchase gasoline or groceries. Fraud can also be perpetrated in the context of electronic transactions. Electronic fraud can be particularly devastating because the perpetrator does not need physical access to a victim’s credit card (or other resource) to perform the fraud. Improved techniques to prevent fraud would be useful. Improved techniques to identify those who commit fraud would also be useful.

IPR2023-00329, APPL-1001

Stone



US 20100042535A1

(19) **United States**
(12) **Patent Application Publication**
Stone

(10) **Pub. No.: US 2010/0042535 A1**
(43) **Pub. Date: Feb. 18, 2010**

Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 10/00 (2006.01)

(52) **U.S. Cl.** **705/39**; 705/1

(57) **ABSTRACT**

Actual currency is shown displayed on a user device, where the currency represents an amount of money selected by the user. For example, if the user selects $86.21 for U.S. Dollars, the display will show four twenty dollar bills, one five dollar bill, one one dollar bill, two dimes, and one penny.

Keep Display

Enter Funding Source

Confirm?

Transfer Funds

APPL-1008
APPLE INC. / Page 1 of 12

CURRENCY DISPLAY

BACKGROUND

[0001] 1. Field of Invention

[0002] The present invention relates to electronic visual displays, and in particular, to such displays that show a visual representation of financial instruments.

DETAILED DESCRIPTION

[0016] Embodiments of the present disclosure enable users to see a selected actual currency representing the amount entered by the user into a device with a display screen. For example, if the user enters $33.26 in U.S. dollars, the display will show one U.S. twenty dollar bill, one U.S. ten dollar bill, three U.S. one dollar bills, one U.S. quarter, and one U.S. penny. This gives the user a visual representation of the amount, which reinforces the value of the amount and provides the user with a more visually rich interface.

POR [17] at 28-29

Stone Is Not Analogous Art

Petitioner's field of endeavor is too broad.

> ***Second***, Stone is not analogous art to the '010 Patent because it is not directed to improved techniques to prevent and detect fraud within electronic transactions. POR, 28. Petitioner's proposed field of endeavor "electronic financial transactions," Pet. 7, is too broad such that it would be beyond what a POSITA would reasonably be expected to look for to find a solution to the problem facing the inventor, i.e., fraud detection. *See* POR, 27.

Sur-Reply [20] at 24

Stone and Hoyos Teach Away from Each Other

No motivation to combine where reference teaches away.

> "There is no suggestion to combine, however, if a reference teaches away from its combination with another source."

Tec Air, Inc. v. Denso Mfg. Mich. Inc., 192 F.3d 1353, 1360 (Fed. Cir. 1999)

POR [17] at 29

Stone and Hoyos Teach Away from Each Other

A reference teaches away if a POSITA would led in a direction divergent to path taken by the applicant.

> "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."

In re Urbanski,
809 F.3d 1237, 1244 (Fed. Cir. 2016)

POR [17] at 29-30, 38

Stone and Hoyos Teach Away from Each Other

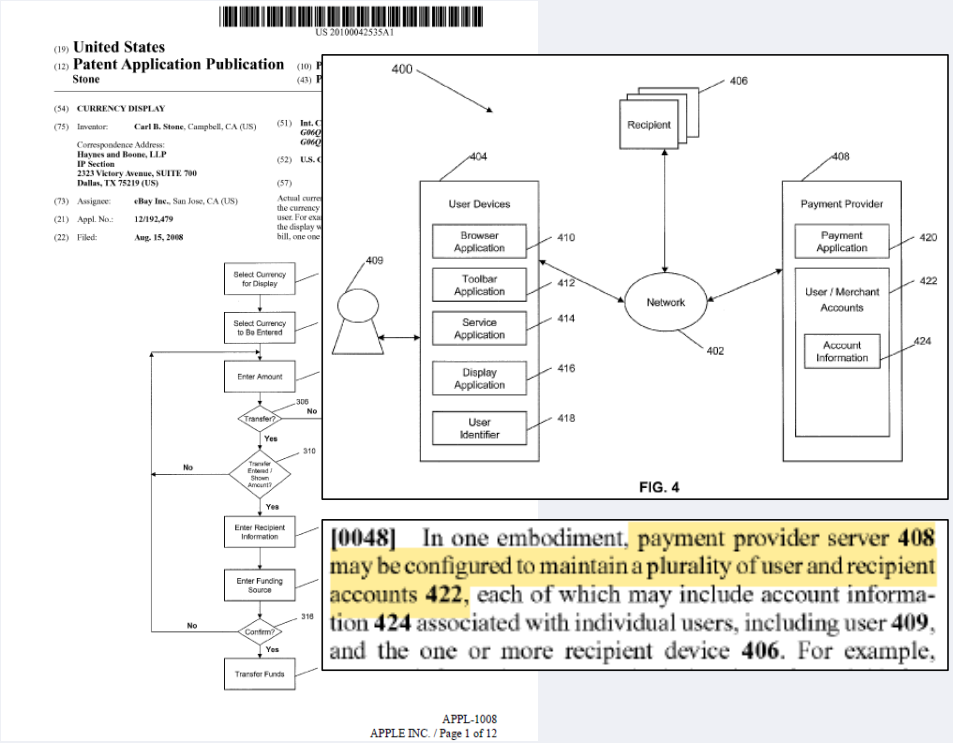
Stone and Hoyos require incompatible computing environments.

> ***Third***, Stone and Hoyos teach away from each other such that a POSITA would not have thought to combine their teachings because they require incompatible computing environments. POR, 29-34; Ex. 2032 ¶¶ 77-83. The

Sur-Reply [20] at 24-25

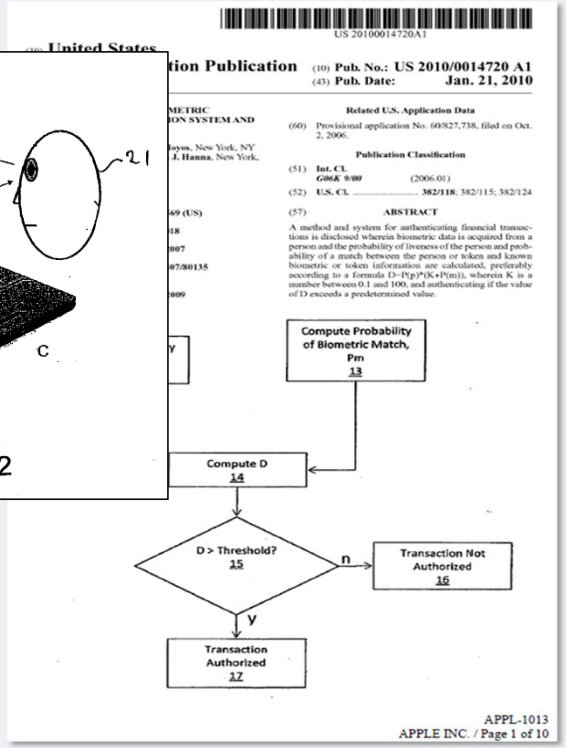
Stone and Hoyos Teach Away from Each Other

Stone



Server

Hoyos



Client

Ex. 1008, Ex. 1013

Stone and Hoyos Teach Away from Each Other

A POSITA starting with Stone would not implement Hoyos' client-side authentication techniques.

A POSITA starting with Stone would understand a server structure is required and would not consider implementing local (client-side) fraud detection techniques like those disclosed in Hoyos. POR, 31-32; Ex. 2032 ¶¶ 80-81. For one, local authentication would be redundant. *Id.* All user account information for processing transactions is stored on the payment server. Ex. 1008, [0045]-[0046]. Storing the same user account information on the user device would be a waste of device storage—antithetical to using a remote server. *Id.* Besides, local authentication can be problematic given variance among user devices in security, processing power, camera resolution, and biometric capabilities. Running computationally intensive biometric analysis locally could lead to performance bottlenecks, especially on older or lower-end devices. *See, e.g.*, Ex. 1038, 64 (Systems using client-side matching "are not secure if the client device is not trusted; therefore additional cryptographic support is needed.").

Sur-Reply [20] at 25

Stone and Hoyos Teach Away from Each Other

A POSITA would not be motivated to implement Hoyos over a remote server.

Nor would a POSITA implement Hoyos' techniques over a remote server. POR, 32-33; Ex. 2032 ¶¶ 81-83. Hoyos does not disclose any remote server applications. It discloses its techniques are performed locally on a computer, connected to a camera. *See, e.g.*, Ex. 1013, [0018]-[0020], cls. 5-7, 13, 17-18. Employing Hoyos' techniques over a remote server would also undermine the benefits of local authentication that Petitioner associates with Hoyos. *See* Ex. 1003 ¶ 68. For instance, it would increase latency by requiring communication with a server and decrease privacy and security of user information by requiring transfer of sensitive data over a network. *See* POR 33; Ex. 2032, ¶¶ 81-83.

Sur-Reply [20] at 25

Fraud Reduction Patents

No Motivation to Combine Stone-FFIEC Guidance

No Motivation to Combine Stone-FFIEC Guidance

Petitioner's Alleged Motivation to Combine
Is Conclusory and Unsupported

Petitioner's assertions are conclusory and provide no actual explanation for *why* a POSITA would have combined Stone and the Guidance. Again, Petitioner presumes that Stone had a need for authentication for fraud detection. But Stone is not concerned with security of transactions. It is concerned with providing an improved display for the user and "richer interface" that provides a currency display. Ex. 1008 at [0016]. Stone also does not view fraud as a problem that needs to be addressed, with increased security, nor does it even mention electronic payment fraud. *See supra* III.A.1.c. In fact, it is telling that whenever Petitioner states the proposition that Stone had a need for fraud detection, Petitioner never once cites the Stone reference. *See, e.g.*, Pet. at 69; *see also* Ex. 2032 ¶ 96.

POR [17] at 43

No Motivation to Combine Stone-FFIEC Guidance

The Guidance is outside a POSITA's area of interest.

A POSITA also would not have combined Stone with the FFIEC Guidance because the Guidance is outside a POSITA's area of interest as defined by Petitioner. A reference is considered publicly accessible if "persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Samsung Elecs. Co., Ltd. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019). Petitioner has defined a POSITA as one holding "a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent." *See* Section II.C. An engineer fitting this description and exercising reasonable diligence would not have been inclined to look to high-level and non-technical regulatory guidance directed to the banking industry to develop precise technical solutions for electronic fraud. *See* Ex. 2032 ¶ 98.

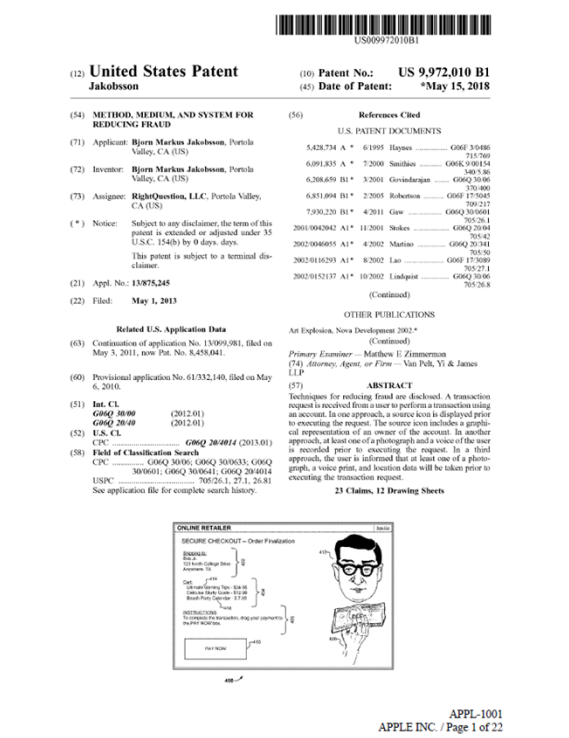
POR [17] at 44

IPR2023-00329
U.S. Patent No. 9,972,010

Limitations [1.2]-[1.5]: Stone-Hoyos does not disclose or render obvious the “virtual likeness of the face of the account holder.”

Limitations [1.2]-[1.5] – "Virtual Likeness"

'010 Patent



US009972010B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 9,972,010 B1**
(45) **Date of Patent: *May 15, 2018**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days. days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/875,245**

(22) Filed: **May 1, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/069,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/4014*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 30/06; G06Q 30/0633; G06Q 30/0601; G06Q 30/0641; G06Q 20/4014
USPC 705/26.1, 27.1, 26.81
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A *	6/1995	Haynes	G06F 3/0486 715/769
6,091,835	A *	7/2000	Smithies	G06K 9/00154 340/5.86
6,208,659	B1 *	3/2001	Govindarajan	G06Q 30/06 370/400
6,851,094	B1 *	2/2005	Robertson	G06F 17/5045 709/217
7,930,220	B1 *	4/2011	Gaw	G06Q 30/0601 705/26.1
2001/0042042	A1 *	11/2001	Stokes	G06Q 20/04 705/42
2002/0046055	A1 *	4/2002	Martino	G06Q 20/341 705/50
2002/0116293	A1 *	8/2002	Lao	G06F 17/3089 705/27.1
2002/0152137	A1 *	10/2002	Lindquist	G06Q 30/06 705/26.8

(Continued)

OTHER PUBLICATIONS

Art Explosion, Nova Development 2002.*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets

APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00329, APPL-1001

a) Stone-Hoyos does not disclose Limitations [1.2]-[1.5].[1]

Independent claim 1 of the '010 Patent claims a system, comprising:

[1.1] one or more processors configured to:

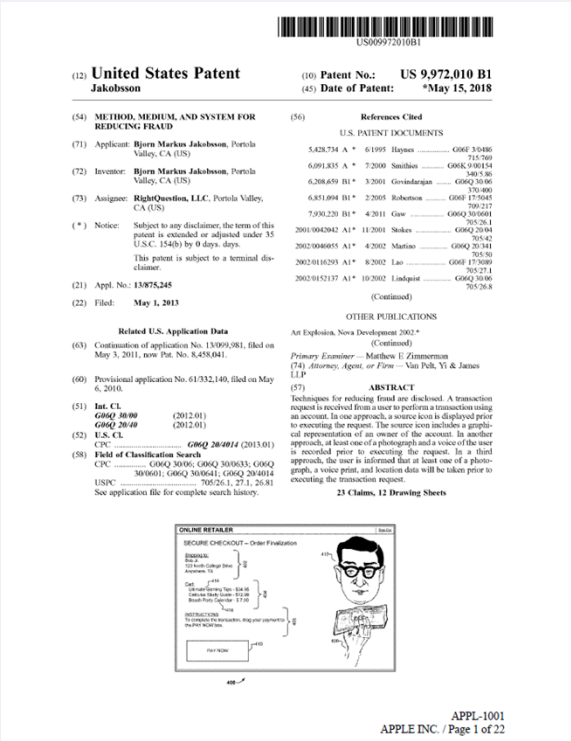
[1.2] receive a virtual likeness of a face of an account holder; associate, in a data store, ***the virtual likeness of the face of the account holder*** with an account of the account holder;

[1.3] render, in an interface, ***the virtual likeness of the face of the account holder***;

Sur-Reply [20] at 2

Must Be the *Same* "Virtual Likeness"

'010 Patent



US009972010B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 9,972,010 B1**
(45) **Date of Patent: *May 15, 2018**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days. days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/875,245**

(22) Filed: **May 1, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/069,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/4014*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 30/06; G06Q 30/0633; G06Q 30/0601; G06Q 30/0641; G06Q 20/4014
USPC 705/26.1, 27.1, 26.81
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A *	6/1995	Haynes	G06F 3/0486 715/769
6,091,835	A *	7/2000	Smithies	G06K 9/00154 340/5.86
6,208,659	B1 *	3/2001	Govindarajan	G06Q 30/06 370/400
6,851,094	B1 *	2/2005	Robertson	G06F 17/5045 709/217
7,930,220	B1 *	4/2011	Gaw	G06Q 30/0601 705/26.1
2001/0042042	A1 *	11/2001	Stokes	G06Q 20/04 705/42
2002/0046055	A1 *	4/2002	Martino	G06Q 20/341 705/50
2002/0116293	A1 *	8/2002	Lao	G06F 17/3089 705/27.1
2002/0152137	A1 *	10/2002	Lindquist	G06Q 30/06 705/26.8

(Continued)

OTHER PUBLICATIONS

Art Explosion, Nova Development 2002.*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets

APPL-1001
APPLE INC. / Page 1 of 22

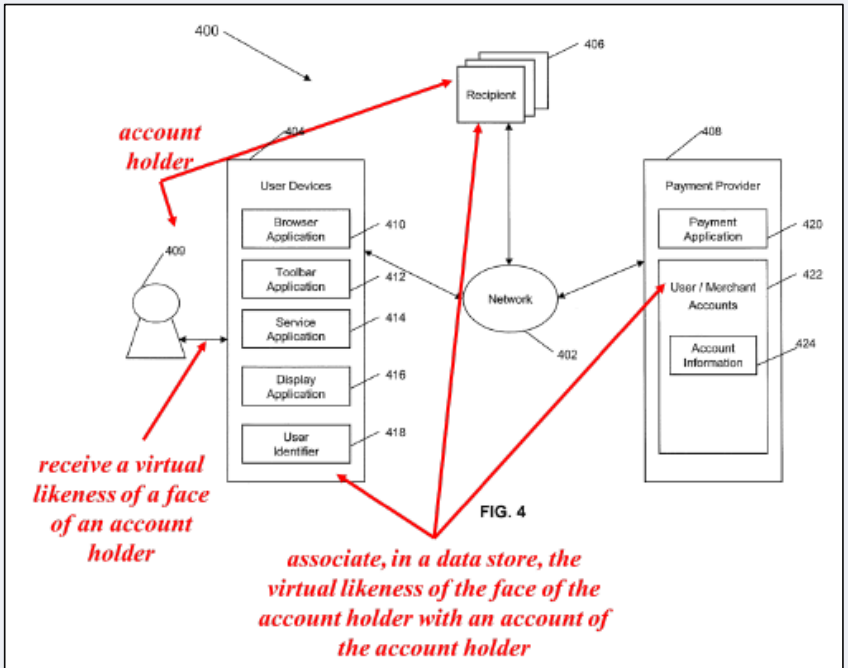
IPR2023-00329, APPL-1001

> Petitioner in its reply does not dispute that for claim 1 of the '010 Patent, the antecedent-basis rule for claim drafting requires the *same* "virtual likeness of the face of the account holder" is received, associated in a data store with an account of an account holder, and rendered in an interface. *See* Pet. Reply, 2-3. That said, the

Sur-Reply [20] at 2-3

Petition Doesn't Identify *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Receive & Associate



APPL-1008, FIG. 4, annotated

Render in an Interface

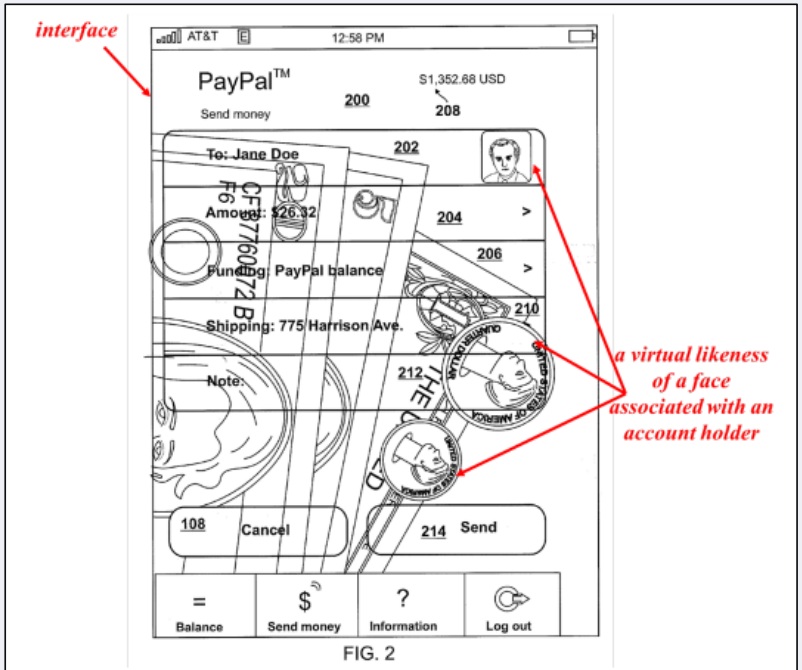


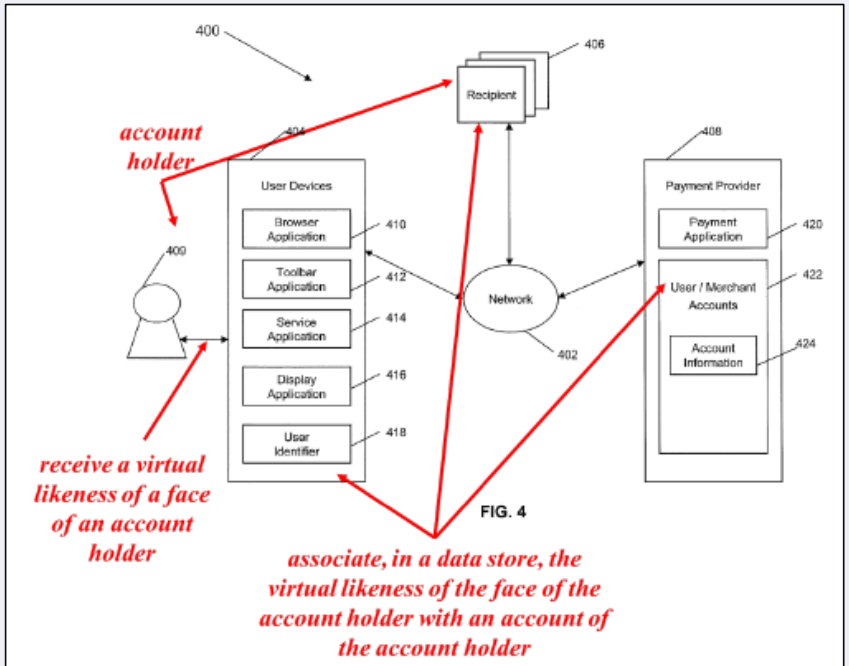
FIG. 2

APPL-1008, FIG. 2, annotated (see also FIG. 1)

Petition [2] at 26-31

Petition Doesn't Identify *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Receive & Associate



APPL-1008, FIG. 4, annotated

Second, Stone describes associating, using user identifier 418, in a data store (storage component 508 of user devices 404 alone, or in combination with storage component 508 of other devices including payment provider server 408), the virtual likeness of the face (photo) of the account holder (user 409) with an account (user account 422) of the account holder (user 409). APPL-1008, [0045] ("In various implementations, **user identifier 418** [including photograph image of the user] 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."); [0048] ("payment provider server 408 may be configured to

[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**.

Petition [2] at 28; Ex. 1008

Petition Doesn't Identify *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Render in an Interface

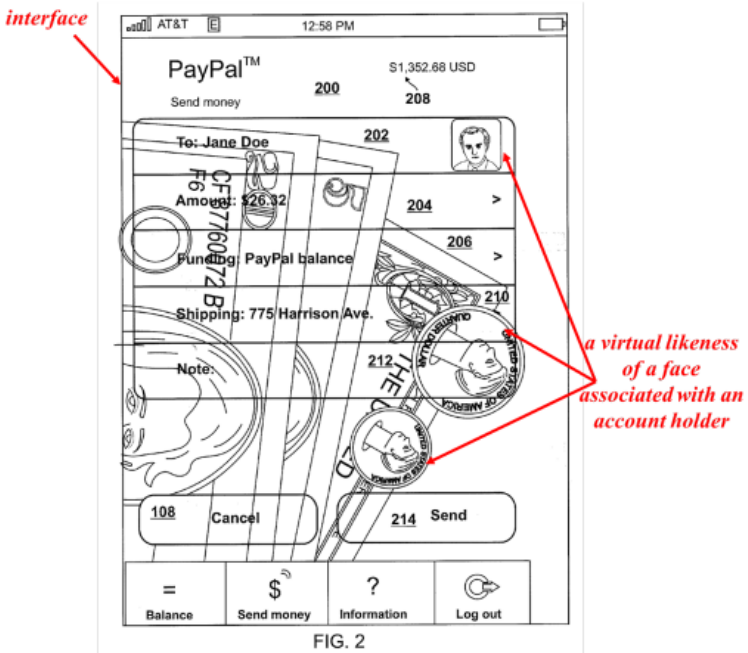


FIG. 2

APPL-1008, FIG. 2, annotated (see also FIG. 1)

Petition never identifies that recipient photo and personalized currency photo are "*associated*" with an account of an account holder.

But, as mentioned above, the Petition never identifies either the recipient photo 202 or the personalized currency display for the *receive* or *associate* limitations of [1.2]. *See* Pet., 26-28. Therefore, the Board should ignore Petitioner's untimely examples asserted for the first time in its reply and hold Petitioner to the Grounds as asserted in the Petition, which fail on their face. *Axonics, Inc. v. Medtronic, Inc.*, 75 F.4th 1374, 1380 (Fed. Cir. 2023) (Petitioner "may not submit new evidence or argument in reply that it could have presented earlier, e.g. to make out a prima facie case of unpatentability." (quoting U.S. Patent Trial and Appeal Board, Consolidated Trial Practice Guide 73 (Nov. 2019)).

Petitioner is foreclosed from now arguing that recipient or currency photos meet the association limitation.

Sur-reply [20] at 6; Petition [2] at 30

Stone Doesn't Disclose the *Same* Virtual Likeness that Meets the Receive, Associate, and Render Limitations

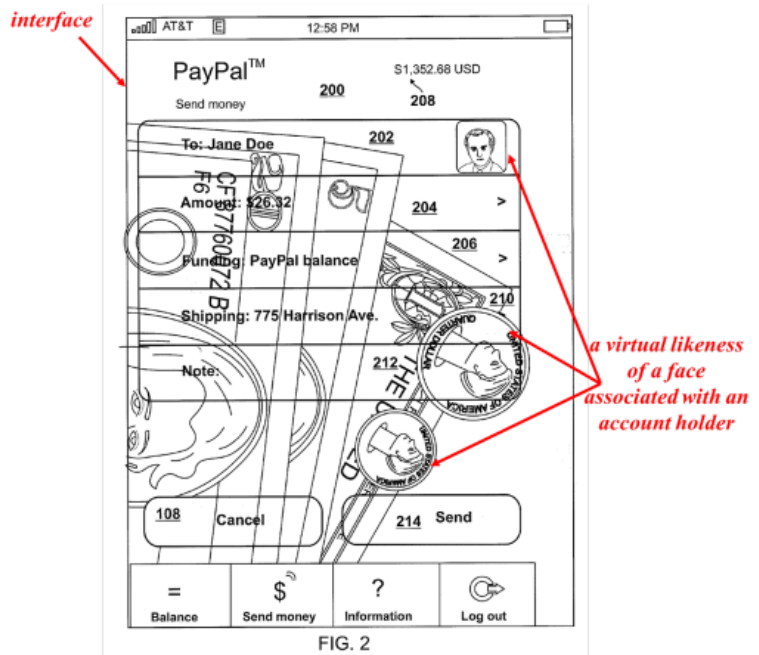


FIG. 2

APPL-1008, FIG. 2, annotated (see also FIG. 1)

Stone only discloses user identifier 418 as being "*associated*" with a user account.

[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**.

Sur-reply [20] at 6; Petition [2] at 30; Ex. 1008

Stone Doesn't Disclose the *Same* Virtual Likeness that Meets the Receive, Associate, and Render Limitations

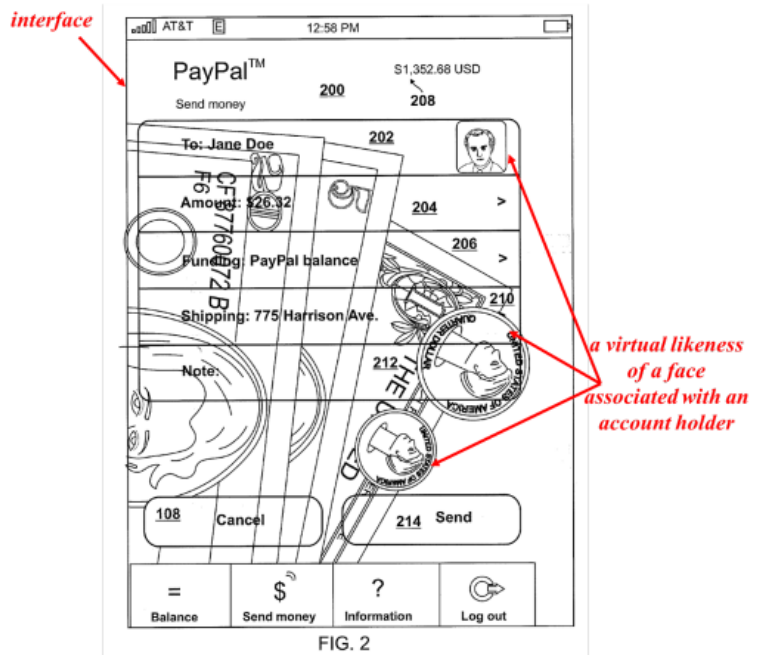


FIG. 2

APPL-1008, FIG. 2, annotated (see also FIG. 1)

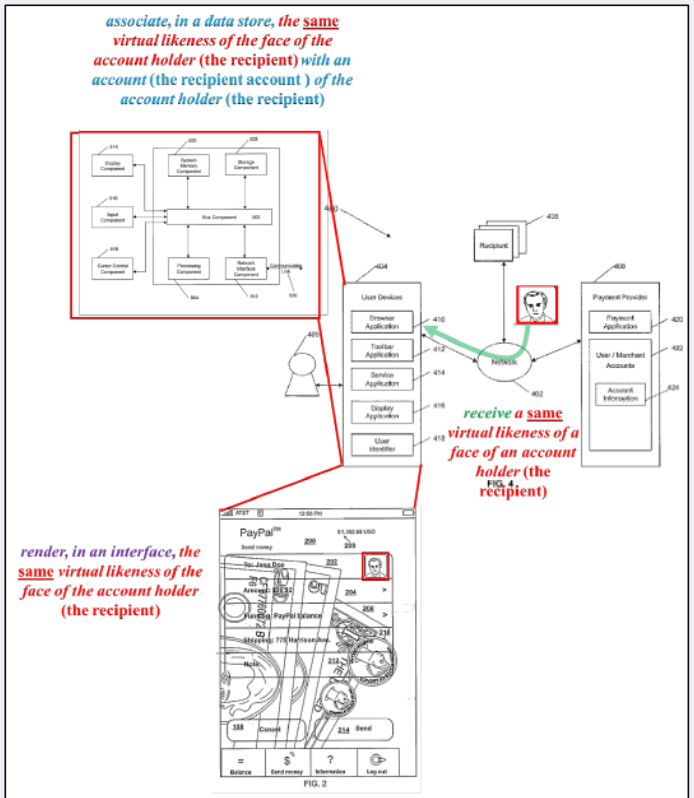
Recipient photo and currency photo are not the same as or related to user identifier 418.

[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**.

Sur-reply [20] at 6; Petition [2] at 30

Examples in Petitioner's Reply Fail to Identify the *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Petitioner's Example 1.1 (Recipient Photo 202, Client-Side Single Processor)



Example 1.1 of Stone Combined with Hoyos
(annotated based on APPL-1008, Stone, FIGS. 2 and 4).

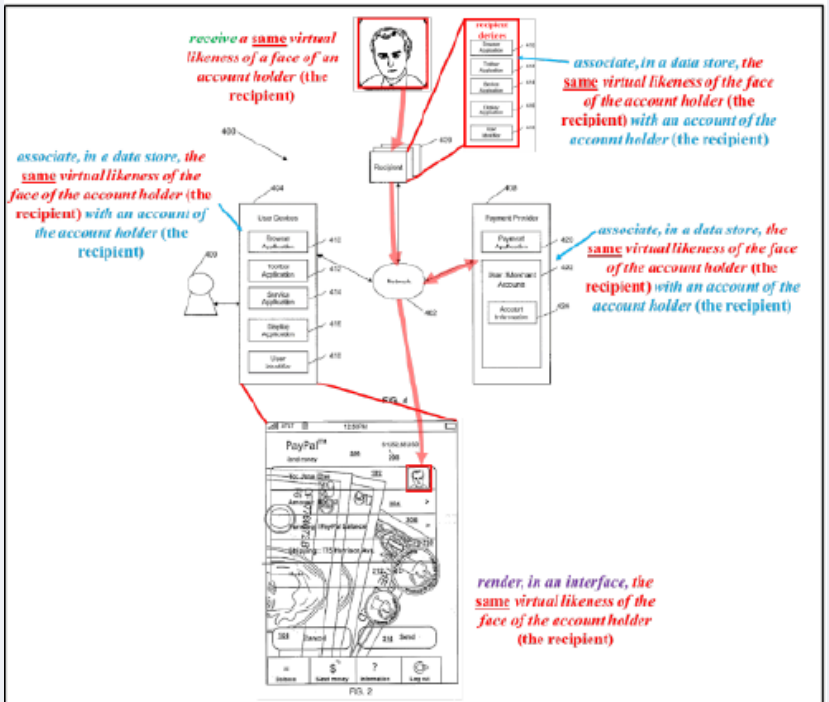
No association of recipient photo.

and the recipient's account, but nothing in the Stone reference states that any association of recipient account information occurs in any component of the user device shown in Figure 5. The only association of users with specific account information disclosed in Stone occurs on the payment provider server 408 and the association is between user identifier 418 and the user account 422, not recipient photo 202. *See* Ex. 1008, [0045]-[0046]; POR, 18; Ex. 2032 (Dr. Goodrich Declaration) ¶¶ 57-58.

Sur-reply [20] at 7-11

Examples in Petitioner's Reply Fail to Identify the *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Petitioner's Example 1.2 (Recipient Photo 202, Server Multiple Processors)



Example 1.2 of Stone Combined with Hoyos (annotated based on APPL-1008, Stone, FIGS. 2 and 4).

No association of recipient photo; can't point to multiple processors.

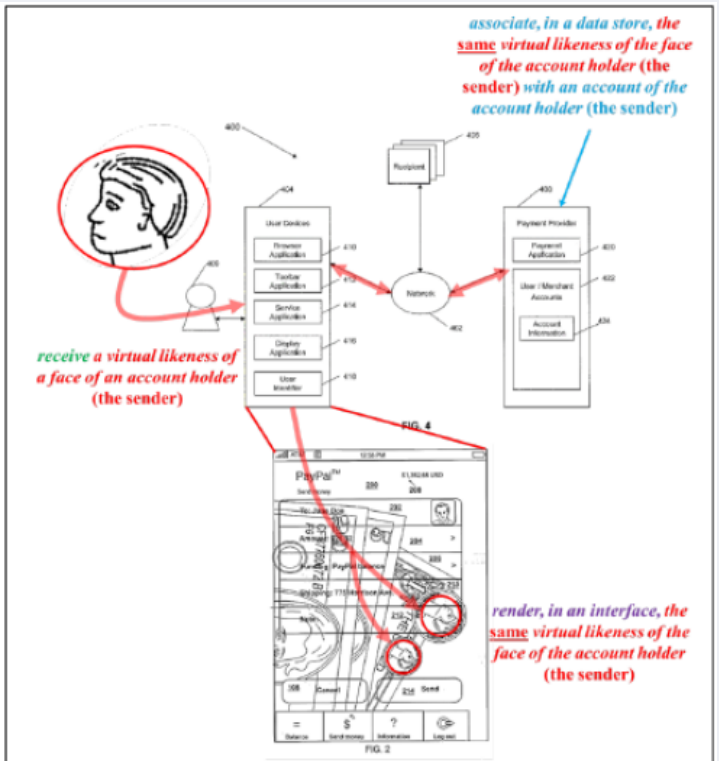
Petitioner's Example 1.2 relies on recipient photo 202 as disclosing the "virtual likeness of the face of the account holder" limitations of the '010 Patent's independent claims using three different processors: the recipient device processor 406 (receive element), the recipient device processor 406 and payment provider server 408 (associate element), and the user device processor 404 (render-in-the-interface element). *See* Pet. Reply, 9. But as with Petitioner's example 1.1, Stone does not disclose that the recipient photo is ever associated with a recipient account on the recipient device or the payment provider server. The only association of user

Additionally, combining functionality of multiple processors to disclose the virtual likeness limitations does not suffice. While the '010 Patent's claims recite "one or more processors," the Federal Circuit has held for similarly worded claims where there is "a processor" or "one or more processors" configured to perform a series of limitations, there must be *at least one* processor capable of performing *each of* the claimed functions. *See Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317 (Fed. Cir. 2023) (holding that a claim to "a microprocessor" (meaning "one or more microprocessors") "require[s] that at least one microprocessor be capable of performing each of the claimed functions."). By pointing to multiple processors as

Sur-reply [20] at 11-13

Examples in Petitioner's Reply Fail to Identify the *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Petitioner's Example 2.1 (Currency Image, Client-Side Single Processor)



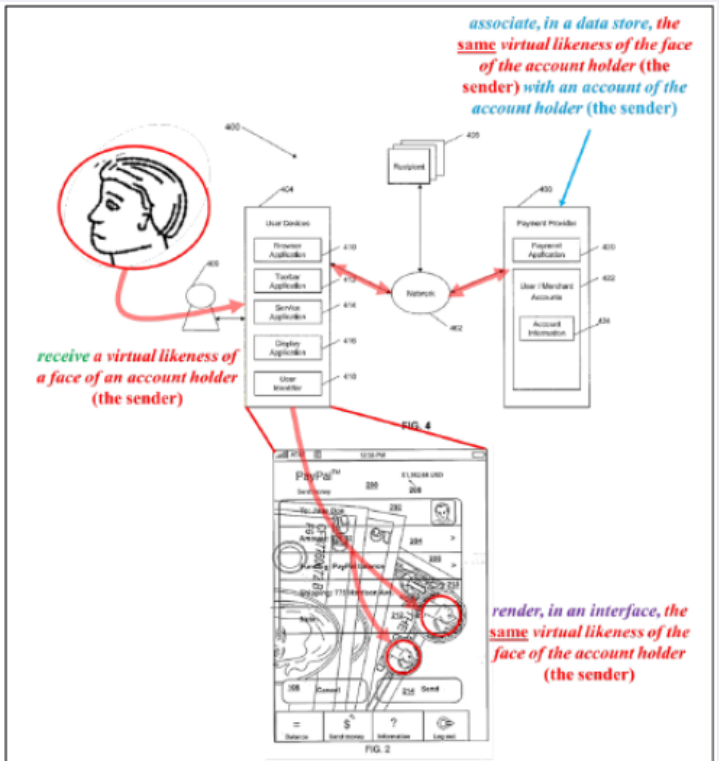
Example 2.2 of Stone Combined with Hoyos (annotated based on APPL-1008, Stone, FIGS. 2 and 4).

No association of currency image.

Sur-reply [20] at 13-16

Examples in Petitioner's Reply Fail to Identify the *Same* Virtual Likeness for the Receive, Associate, and Render Limitations

Petitioner's Example 2.2 (Currency Image, Server Multiple Processors)



Example 2.2 of Stone Combined with Hoyos (annotated based on APPL-1008, Stone, FIGS. 2 and 4).

No association of currency image; can't point to multiple processors.

Sur-reply [20] at 16-18

Fraud Reduction Patents

Stone-Hoyos does not disclose “memory” limitations

“Memory” Limitations

’010 Patent

1. A system, comprising:

one or more processors configured to:

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;

render, in an interface, the virtual likeness of the face of the account holder;

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;

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;

capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

on the captured biometric information, that the user is alive; and

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

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

IPR2023-00329, APPL-1001, ’010 Patent Cl. 1

’656 Patent

1. A system, comprising:

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;

render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;

render, in the one or more interfaces, a transaction icon associated with the electronic transaction;

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;

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

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

transaction, wherein performing the fraud detection analysis comprises:

performing a comparison based at least in part on the stored biometric information and the captured biometric information; and

determining, based at least in part on the captured biometric information, that the user is alive; and

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

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

IPR2023-00330, APPL-1001, ’656 Patent Cl. 1

’886 Patent

1. A system, comprising:

one or more processors configured to:

render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;

subsequent to an interaction by a user with an icon rendered in the one or more interfaces:

capture contextual information comprising location data usable to determine a physical location associated with the user; and

capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and

a memory coupled to the one or more processors and configured to provide the processor with instructions.

part on:

the physical location associated with the user determined using the captured location data; and

an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and

a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

“Memory” Limitations

Limitation [1.9]: “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.”

Petitioner’s client-side model fails.

Petitioner contends that both its client-side and server-side implementation of Stone-Hoyos would render obvious Limitation [1.9]. Pet. Reply, 16-19. Petitioner is wrong.

First, Petitioner’s client-side model fails because it is predicated on Stone’s processor on the user device 404 as being configured to perform all the functionality of the ’010 Patent’s claim 1. But as just explained, the user device processor 404 does not disclose all the limitations of the ’010 Patent’s claim 1, so it cannot be “*the* one or more processors” coupled to “a memory” for limitation [1.9]. *See* Section II.A.1.

Sur-reply [20] at 19

“Memory” Limitations

Limitation [1.9]: “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.”

Petitioner’s server-side model fails.

For the purported server-side implementation of Stone-Hoyos, a POSITA would not have been motivated to implement the biometric authentication techniques of Hoyos within a remote setup as explained below in Section II.A.3.(c) (no motivation to combine Stone and Hoyos). Petitioner also cannot point to multiple processors as disclosing all the limitations the one or more processors must be configured to perform. *See* Section II.A.1.(b); *Salazar*, 64 F.4th at 1317. Additionally, recipient photo 202 and the personalized virtual currency Petitioner relies on for limitation [1.3] (rendering the virtual likeness in an interface) are never associated with a user account in the payment server, meaning neither the recipient photo nor personalized currency display can meet *all* the limitations required of the virtual likeness in the ’010 Patent’s claim 1. *See* Section II.A.1.(b).

But memory 506 fails to disclose the “memory” of the ’010 Patent’s claim 1 because it does not provide instructions to the claimed “one or more processors.” First, memory 506, as Petitioner concedes, only provides instructions to the processor 504 on the user device. Pet. Reply, 18. A POSITA reading claim 1 of the ’010 Patent would understand the plain meaning of “provide the one or more processors with instructions” to include at least the instructions to perform the limitations of claim 1 (e.g., receive, associate in a data store, and render in an interface the virtual likeness of the face of the account holder). *See* Ex. 1050, Goodrich Tr. 59:3-59:8. Stone does not disclose, nor does Petitioner allege, that

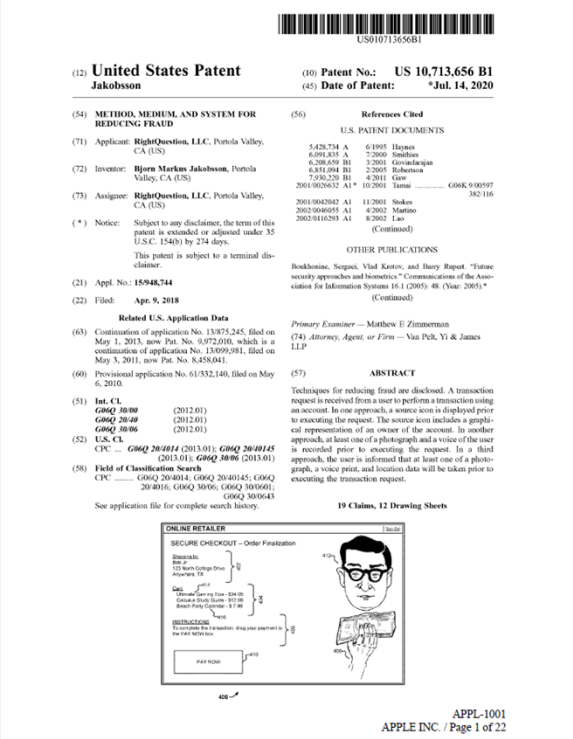
Sur-reply [20] at 19-20

IPR2023-00330
U.S. Patent No. 10,713,656

Limitation [1.2]: Stone-Hoyos-Varghese does not disclose or render obvious "store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder."

’656 Patent Limitation [1.2]

’656 Patent



US010713656B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 10,713,656 B1**
(45) **Date of Patent: *Jul. 14, 2020**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **RightQuestion, LLC**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 274 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/948,744**

(22) Filed: **Apr. 9, 2018**

Related U.S. Application Data

(63) Continuation of application No. 13/875,245, filed on May 1, 2013, now Pat. No. 9,972,010, which is a continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/06 (2012.01)

(52) **U.S. Cl.**
CPC ... ***G06Q 20/4014*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 30/06*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4014; G06Q 20/40145; G06Q 20/4016; G06Q 30/06; G06Q 30/0601; G06Q 30/0643
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A	6/1995	Haynes
6,091,835	A	7/2000	Smithies
6,208,659	B1	3/2001	Govindarajan
6,851,094	B1	2/2005	Robertson
7,930,220	B1	4/2011	Gaw
2001/0026632	A1 *	10/2001	Tamai G06K 9/00597 382/116
2001/0042042	A1	11/2001	Stokes
2002/0046055	A1	4/2002	Martino
2002/0116293	A1	8/2002	Lao

(Continued)

OTHER PUBLICATIONS

Boukhonine, Sergei, Vlad Krotov, and Barry Rupert. "Future security approaches and biometrics." Communications of the Association for Information Systems 16.1 (2005): 48. (Year: 2005).*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

19 Claims, 12 Drawing Sheets

ONLINE RETAILER
SECURE CHECKOUT – Order Finalization
PAY NOW

APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00330, APPL-1001

Claim 1

1. A system, comprising:

1. A system, comprising:

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;

associated with the electronic transaction;

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;

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;

perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:

performing a comparison based at least in part on the stored biometric information and the captured biometric information; and

determining, based at least in part on the captured biometric information, that the user is alive; and

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

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

IPR2023-00330, APPL-1001, ’656 Patent Cl. 1

Stone Does Not Disclose Any Association between User Identifier 418 and a User Account that Occurs on a User Device

2. Stone-Hoyos-Varghese does not disclose or render obvious "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" as recited in limitation [1.2].[1]

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, where all user account information is stored. Ex. 1008 at [0045]-[0046]. In the Petition, Petitioner appears to identify the payment provider server 408 as "associating" the user identifier with user account 422.

Sur-reply [20] at 11

Stone Does Not Disclose Any Association between User Identifier 418 and a User Account that Occurs on a User Device

Limitation [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"

Association must occur on the *same* processor that receives, stores and associates the use biometric with a user account.

> Pet., 33. But association of the user identifier with a user account on the payment provider server cannot disclose [1.2]. The association of the user biometric (user identifier 418) with an account must occur on the *same* processor that receives, stores, and associates the user biometric (user identifier 418) with a user account. *See Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317 (Fed. Cir. 2023) (holding that a claim to "a microprocessor" (meaning "one or more microprocessors") "require[s] that at least one microprocessor be capable of performing each of the claimed functions.").

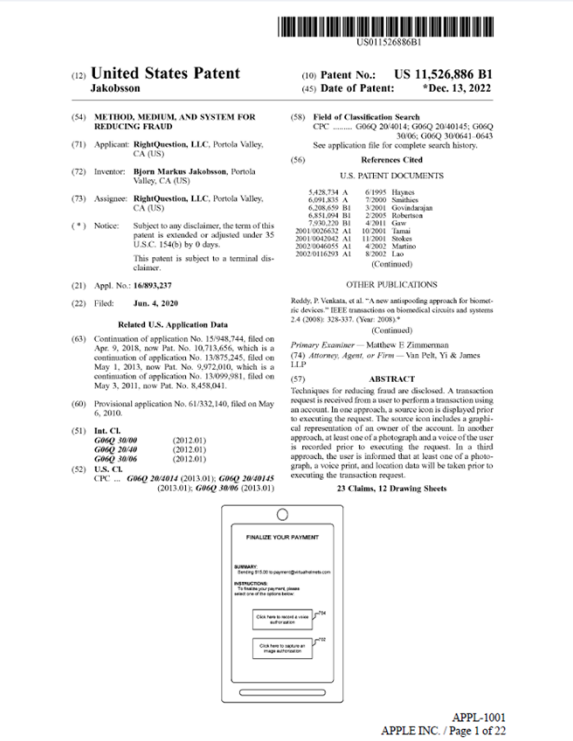
Sur-reply [20] at 12

IPR2023-00331
U.S. Patent No. 11,526,886

Limitation [1.2.2]: Stone-Hoyos-Varghese does not render obvious “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment.”

’886 Patent Limitation [1.2.2]

’886 Patent



US011526886B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 11,526,886 B1**
(45) **Date of Patent: *Dec. 13, 2022**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **RightQuestion, LLC**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/893,237**

(22) Filed: **Jun. 4, 2020**

Related U.S. Application Data

(63) Continuation of application No. 15/948,744, filed on Apr. 9, 2018, now Pat. No. 10,713,656, which is a continuation of application No. 13/875,245, filed on May 1, 2013, now Pat. No. 9,972,010, which is a continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/06 (2012.01)

(52) **U.S. Cl.**
CPC ... ***G06Q 20/4014*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 30/06*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4014; G06Q 20/40145; G06Q 30/06; G06Q 30/0641.0643
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A	6/1995	Haynes
6,091,835	A	7/2000	Smithies
6,208,659	B1	3/2001	Govindarajan
6,851,094	B1	2/2005	Robertson
7,930,220	B1	4/2011	Gew
2001/0026632	A1	10/2001	Tamai
2001/0042042	A1	11/2001	Stokes
2002/0046055	A1	4/2002	Martino
2002/0116293	A1	8/2002	Lao

(Continued)

OTHER PUBLICATIONS

Reddy, P. Venkata, et al. "A new antispoofing approach for biometric devices." IEEE transactions on biomedical circuits and systems 2.4 (2008): 328-337. (Year: 2008).*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets

FINALIZE YOUR PAYMENT

APPL-1001
APPLE INC. / Page 1 of 22

IPR2023-00331, APPL-1001

Claim 1

1. A system, comprising:
one or more processors configured to:
render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
capture contextual information comprising location data usable to determine a physical location associated with the user; and
capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
the physical location associated with the user determined using the captured location data; and
an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and
a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

Stone Does Not Disclose an Enrollment Process

2. Stone-Hoyos-Varghese does not render obvious "wherein the virtual likeness of the face was selected by the account holder as part of an enrollment" as recited in limitation [1.2.2].[1]

Claim 1 of the '886 Patent claims "one or more processors configured to: render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment." Ex. 1001 at cl. 1. Based on this claim structure, *the* virtual likeness rendered in the interface and selected during enrollment must be the *same* virtual likeness. *See NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1306 (Fed. Cir. 2005) (noting use of "a" followed by use of "the" indicates reference to the same "destination processor"). The Petition does not identify, and Stone does not disclose, a virtual likeness of a face of an account holder that is both rendered in an interface and selected as part of an enrollment process. For the likeness rendered in the interface, Petitioner points to the personalized currency display on the sender's device (below left) and the recipient photo 202 (below right).

Sur-reply [20] at 12

Petitioner Does Not Disclose that a Recipient Photo Is Selected during an Enrollment Process

As shown in FIGS. 2 and 4 below, Stone as applied in Stone combined with Hoyos and Varghese discloses *an enrollment* or registration procedure (the procedure for establishing a recipient account of the recipient with payment server), where the recipient image displayed on FIG. 2 was selected by the recipient during the enrollment/registration for display. APPL-1008, Stone, [0046] ("Each of the one or more recipient may need to **establish an account** with payment provider server 408 so that payment server provider 408 is able to process money transfers from user 409 with payment provider server"). A POSITA would have understood that such a selected recipient image, which is associated with the recipient account so established, can be stored on the recipient device 406 and/or the payment provider server 408, and would be provided through network 402 such that "user device 404 may be able to access recipient attributes, such as icon information, for display or use by user device 404." APPL-1008, Stone, [0046]; APPL-1056, ¶22.

Petitioner's Reply [19] at 11

IPR2023-00331
U.S. Patent No. 11,526,886

Limitation [1.3.1]: Stone-Hoyos-Varghese does not disclose or render obvious "subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capture contextual information comprising location data."

’886 Patent Limitation [1.3.1]

’886 Patent

US011526886B1

(12) **United States Patent**
Jakobsson

(10) **Patent No.: US 11,526,886 B1**
(45) **Date of Patent: *Dec. 13, 2022**

(54) **METHOD, MEDIUM, AND SYSTEM FOR REDUCING FRAUD**

(71) Applicant: **RightQuestion, LLC**, Portola Valley, CA (US)

(72) Inventor: **Bjorn Markus Jakobsson**, Portola Valley, CA (US)

(73) Assignee: **RightQuestion, LLC**, Portola Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/893,237**

(22) Filed: **Jun. 4, 2020**

Related U.S. Application Data

(63) Continuation of application No. 15/948,744, filed on Apr. 9, 2018, now Pat. No. 10,713,656, which is a continuation of application No. 13/875,245, filed on May 1, 2013, now Pat. No. 9,972,010, which is a continuation of application No. 13/099,981, filed on May 3, 2011, now Pat. No. 8,458,041.

(60) Provisional application No. 61/332,140, filed on May 6, 2010.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/06 (2012.01)

(52) **U.S. Cl.**
CPC ... ***G06Q 20/4014*** (2013.01); ***G06Q 20/40145*** (2013.01); ***G06Q 30/06*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/4014; G06Q 20/40145; G06Q 30/06; G06Q 30/0641.0643
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,428,734	A	6/1995	Haynes
6,091,835	A	7/2000	Smithies
6,208,659	B1	3/2001	Govindarajan
6,851,094	B1	2/2005	Robertson
7,930,220	B1	4/2011	Gew
2001/0026632	A1	10/2001	Tamai
2001/0042042	A1	11/2001	Stokes
2002/0046055	A1	4/2002	Martino
2002/0116293	A1	8/2002	Lao

(Continued)

OTHER PUBLICATIONS

Reddy, P. Venkata, et al. "A new antispoofing approach for biometric devices." IEEE transactions on biomedical circuits and systems 2.4 (2008): 328-337. (Year: 2008).*

(Continued)

Primary Examiner — Matthew E Zimmerman
(74) *Attorney, Agent, or Firm* — Van Pelt, Yi & James LLP

(57) **ABSTRACT**

Techniques for reducing fraud are disclosed. A transaction request is received from a user to perform a transaction using an account. In one approach, a source icon is displayed prior to executing the request. The source icon includes a graphical representation of an owner of the account. In another approach, at least one of a photograph and a voice of the user is recorded prior to executing the request. In a third approach, the user is informed that at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request.

23 Claims, 12 Drawing Sheets

APPL-1001
APPLE INC. / Page 1 of 22

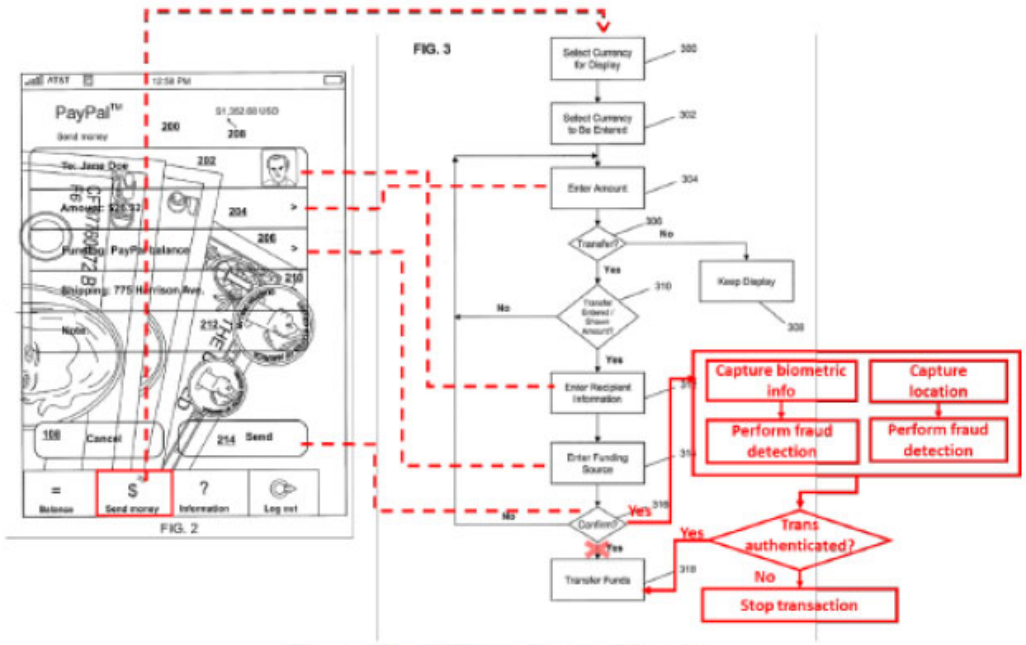
IPR2023-00331, APPL-1001

Claim 1

1. A system, comprising:
one or more processors configured to:
render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
capture contextual information comprising location data usable to determine a physical location associated with the user; and
capturing, using a camera, a set of images; and
facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
the physical location associated with the user determined using the captured location data; and
an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and
a memory coupled to the one or more processors and configured to provide the processor with instructions.

IPR2023-00331, APPL-1001, ’886 Patent Cl. 1

Petitioner's Stone-Hoyos-Varghese Transaction Model



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

Pet., 38.

Petitioner [2] at 38

Varghese Pre-Authentication v. Post-Authentication

Varghese

US 20060282660A1

(19) **United States**

(12) **Patent Application Publication**

Varghese et al.

(10) **Pub. No.: US 2006/0282660 A1**

(43) **Pub. Date: Dec. 14, 2006**

(54) **SYSTEM AND METHOD FOR FRAUD MONITORING, DETECTION, AND TIERED USER AUTHENTICATION**

(76) Inventors: **Thomas Emmanual Varghese**, San Mateo, CA (US); **Jon Bryan Fisher**, Tiburon, CA (US); **Steven Lucas Harris**, Foster City, CA (US); **Don Bosco Durai**, Fremont, CA (US)

Correspondence Address:
WINSTON & STRAWN LLP
1700 K STREET, N.W.
WASHINGTON, DC 20006 (US)

(21) Appl. No.: **11/412,997**

(22) Filed: **Apr. 28, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/676,141, filed on Apr. 29, 2005.

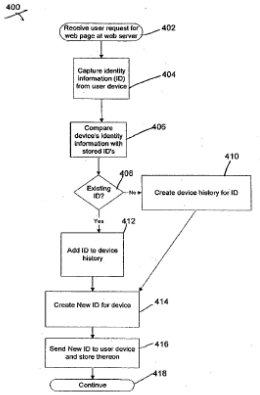
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/155**

(57) **ABSTRACT**

The present invention provides systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices. User devices are identified with fingerprinting information, and their associated risks of fraud are determined from past experience with the device or with similar devices and from third party information. In preferred embodiments, different graphical user interfaces are presented based on both fraud risk and, in the case of a known user, usability. In preferred embodiments, this invention is implemented as a number of communicating modules that identify user devices, assess their risk of fraud, present selected user interfaces, and maintain databases of fraud experiences. This invention also includes systems providing these authentication services.



APPL-1010
APPLE INC. / Page 1 of 50

[0065] This invention generally provides systems and methods that interface with service providing systems of online service providers and assists them in authenticating their user requests, especially user log on requests and transaction sequences (referred to herein as a user's "workflow"). Briefly, this invention authenticates a user and a login request (referred to herein as "pre-authentication") in a manner determined both by the identity of the device from which the authentication request originates this invention as well as by available information concerning the identity of the requesting user. User workflow sequences are authenticated (referred to herein as "post-authentication") using a user's transaction history. In both applications, the precise authentication processes and decisions can be directed by rules from the service provider.

[0074] Authentication services are invoked when a server application or services provider computer system receives user request 1320 that needs authentication. In the case of pre-authentication, the most common user request is a login request to access an application or system. Other requests usually handled by post-authentication services include, e.g., transaction requests involving large amounts of money. User requests can be received directly from communication subsystems, or alternatively, can be forwarded from the service provider application or system across an interface to the authentication processes.

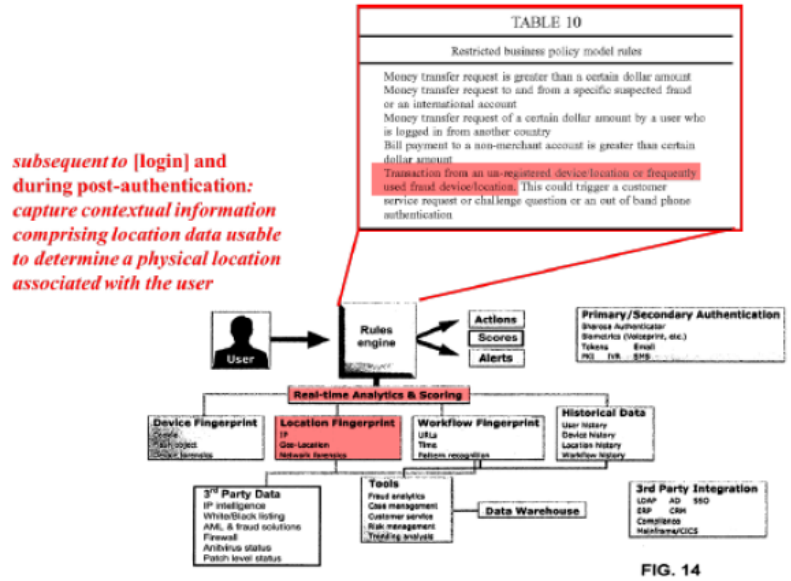
[0075] In preferred embodiments, authentication services can be invoked through an externally available application programming interface ("API"). Table 1 list a selection of exemplary API requests.

Ex. 1010 (Varghese)

No Evidence of Post-Authentication Location Capture Post-Authentication

Petitioner's Transaction Model Fails

Petitioner points to Figure 14 together with Table 10 and [0109] from Varghese as supposedly showing the disclosure of the post-authentication (in-transaction) location capture.



APPL-1010, Varghese, FIG. 14 and Table 10, annotated.

Pet. Reply, 17.

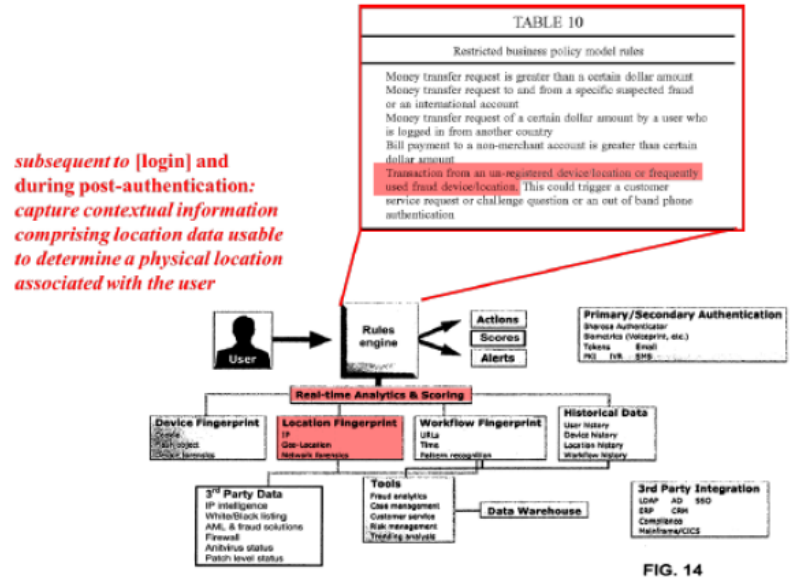
Sur-reply [20] at 17-18

No Evidence of Post-Authentication Location Capture Post-Authentication

Petitioner's Transaction Model Fails

Surreply at 18:

But there are several problems with Petitioner's diagram. First, Table 10 does not coincide with Figure 14 (preferred function configuration). It is associated with Figure 15.B (exemplary policy set and security model). *See* Ex. 1010, [0102]-[0111]. Table 10's rule restricting a "money transfer request of a certain dollar amount by a user who is logged in from another country" also suggests that this rule and Varghese's other security rules apply location data that was already collected at login, not location data collected when a transaction was confirmed, as Petitioner's transaction model requires, *see* Pet., 38.



APPL-1010, Varghese, FIG. 14 and Table 10, annotated.

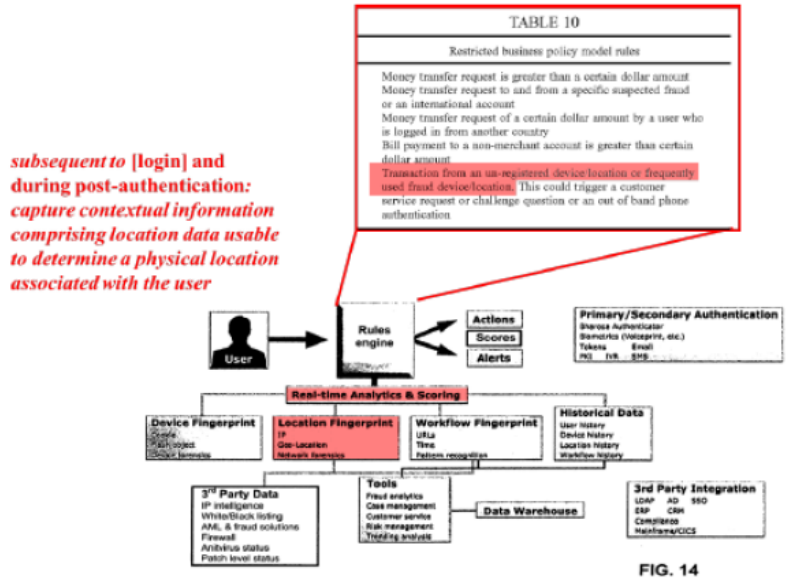
Pet. Reply, 17.

No Evidence of Post-Authentication Location Capture Post-Authentication

Petitioner's Transaction Model Fails

Surreply at 19:

Paragraph 103 and Table 6A of Varghese, like paragraph 109 and Table 10 cited by Petitioner, are both associated with Figure 15.B's security policies. *See* Ex. 1010, [102]-[114]. Both discuss the use of location information within security policies and both address location associated with *user login*, indicating the login is the relevant collection point for location data, not the transaction confirmation step as Petitioner's Stone-Hoyos-Varghese model mandates. Petitioner's reply ignores these sections of Varghese. For this reason and those already discussed, Petitioner's Ground 1 fails to establish that the '656 Patent's Challenged Claims would have been obvious.



APPL-1010, Varghese, FIG. 14 and Table 10, annotated.

Pet. Reply, 17.

No Evidence of Post-Authentication Location Capture Post-Authentication

Petitioner's Transaction Model Fails

Surreply at 20:

[0103] The security policy contains models involving decisions based on risk patterns associated with user, device and location information. The security models are based on known risk conditions and potentially risky behavior and are categorized into the following models. Tables 6A and 6B present illustrative security models.

TABLE 6A

Restricted model	
Location based rules	Logins from restricted countries, (e.g. OFAC countries) Logins from restricted IP addresses Logins from restricted anonymizers and proxies
User based rules	Logins from restricted users list Multiple consecutive failures for the user
Device based rules	Logins from restricted devices Multiple consecutive failures from the device Device using stolen cookies User using the device for the first time

TABLE 6B

Hacker model	
Location based rules	User login from different geographical location (city, state or country) within a given time period Multiple logins from a given IP address within a given time period
User based rules	User login from different geographical location (city, state or country) within a given time period
Device based rules	User login from different device within a given time period Multiple failures from a given device within a given time period Multiple logins from a given device within a given time period Same device used from different geographical location within a given time period

TABLE 10

Restricted business policy model rules

Money transfer request is greater than a certain dollar amount
Money transfer request to and from a specific suspected fraud or an international account
Money transfer request of a certain dollar amount by a user who is logged in from another country
Bill payment to a non-merchant account is greater than certain dollar amount
Transaction from an un-registered device/location or frequently used fraud device/location. This could trigger a customer service request or challenge question or an out of band phone authentication

subsequent to **[login] and during post-authentication:** *capture contextual information comprising location data usable to determine a physical location associated with the user*

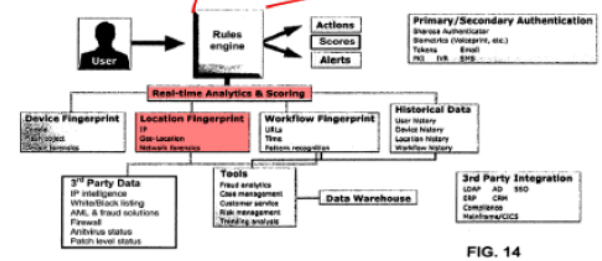


FIG. 14

APPL-1010, Varghese, FIG. 14 and Table 10, annotated.

Pet. Reply, 17.

Table of Contents

Fraud Reduction Patents and Petitioner's References

'010 Patent & Universal Arguments

- No Motivation to Combine Stone and Hoyos.
- No Motivation to Combine Stone and FFIEC Guidance.
- Limitations [1.2]-[1.5]: Stone-Hoyos does not disclose or render obvious the "virtual likeness of the face of the account holder."
- Stone-Hoyos does not disclose "memory" limitations.

'656 Patent

- Limitation [1.2]: Stone-Hoyos-Varghese does not disclose or render obvious "store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder."

'886 Patent

- Limitation [1.2.2]: Stone-Hoyos-Varghese does not render obvious "wherein the virtual likeness of the face was selected by the account holder as part of an enrollment."
- Limitation [1.3.1]: Stone-Hoyos-Varghese does not disclose or render obvious "subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capture contextual information comprising location data."