UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/237,184	09/20/2011	Kenneth P. Weiss	W0537-701320	7352

37462 7590 01/17/2013

LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
CHEUNG, CALVIN K	

ART UNIT	PAPER NUMBER
3662	

NOTIFICATION DATE	DELIVERY MODE
01/17/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelson@LALaw.com

Office Action Summary	Application No.	Applicant(s)	
	13/237,184	WEISS, KENNETH P.	
	Examiner	Art Unit	
	CALVIN CHEUNG	3662	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2012*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,2 and 4-28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,2 and 4-28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This office action is given an identifier, Paper No. 20130103, for reference purposes only.

Status of Claims

2. Claim 3 is cancelled; claims 21-28 are newly added by claim amendments filed 17 December 2012. Therefore, claims 1-2 and 4-28 are examined in this office action.

Response to Arguments

3. Applicant's arguments filed 17 December 2012 have been fully considered but they are not persuasive.

Specification Objection

This objection is withdrawn.

Claim Objection

This objection is withdrawn.

§ 102 Rejection

Applicant argues the Weiss reference "does not teach or suggest the generation of authentication information from the non-predictable value, information derived from at least a portion of the biometric input, and the secret information." The Examiner respectfully disagrees.

Weiss discloses "In one embodiment, …to access the USR database, … retrieves a **secret user code and/**or **time-varying value**…obtains from the user a **secret personal identification code**. … **mathematically combines these three numbers** using a predetermined algorithm to **generate** a one-time **nonpredictable code**…" from ¶ 51. This passage clearly shows that Weiss discloses generating a non-predictable value, information derived from at least a portion of the biometric input, and the secret information. Weiss then discusses about generating authentication information from the nonpredictable value by transmitting the nonpredictable value to another computer, where the nonpredictable code is utilized as authentication information to determine whether a user is granted access (¶ 51).

Applicant repeats the arguments above for claims 15 and 20 and the Examiner traverses these repeated arguments with the same rationale.

§ 103 Rejection

With respect to claim 3, arguments are moot because Applicant has cancelled this claim.

Applicant argues the Weiss reference "does not teach or suggest the generation of authentication information from the non-predictable value, information derived from at least a portion of the biometric input, and the secret information" and includes "Neither Weichert nor Bolle cure this deficiency." In response, Applicant repeats the arguments above for claim 1 and the Examiner traverses these repeated arguments with the same rationale.

Applicant argues the Official Notice used in the rejection of claims 8-12 and requests for documentation to support what is well-known in the art. As requested, the Examiner is now providing the Drexler reference as evidence to support his position for rejecting claims 8 and 9; the Flitcroft reference as evidence to support his position for rejecting claims 10 and 11; and the Krasinski reference as evidence to support his position for rejecting claim 12.

Double Patenting Rejection

This rejection is withdrawn because The Office has approved the Terminal Disclaimer on 21 December 2012.

Claim Objections

4. Claim 21 is objected to because of the following informalities:

Regarding Claim 21, line 3 recites "wherein the of" which is grammatically incorrect. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of 35 U.S.C. 112(b):

> (B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-2 and 4-28 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claim 1 recites an indefinite limitation, "information derived from at least a portion of the biometric input" from lines 14-15. It is unclear whether this limitation is (1) a **new** limitation or (2) making reference to the existing "encrypted authentication information" in line 13. Furthermore, claims 2, 4-14 and 22-24 are rejected based on dependency.

Claims 2, 4-6, 13-14 and 22-24 recite the limitation "The device" in line 1 only. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "The device" in lines 1 and "the device" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "The device" and "the device" in line 1 and "the device" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "The device" in line 1 and "the device" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "the device" in lines 1 and 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "The device" in lines 1 and "the device" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites the limitation "The device" in lines 1 and "the device" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 15 recites an indefinite limitation, "information derived from at least a portion of a biometric data" from lines 10-11. It is unclear whether this limitation is (1) a **new** limitation or (2) making reference to the existing "encrypted authentication information" in line 9. Furthermore, claims 16-19, 21 and 25-26 are rejected based on dependency.

Claim 15 recites the limitation "the device" in lines 3 and 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the device" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation "the device" in lines 1 and 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 18 recites the limitation "the device" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites an indefinite limitation, "information derived from at least a portion of a biometric of the user received by the device" from lines 5-6. It is unclear whether this limitation is (1) a **new** limitation or (2) making reference to the existing "encrypted authentication information" in line 3. Furthermore, claims 27 and 28 are rejected based on dependency.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 4-6 and 13-28 are rejected under 35 U.S.C. 102(b) as being anticipated by US 20020178364 A1 ("Weiss") from IDS.

Regarding Claim 1, Weiss discloses an electronic ID device (e.g., electronic ID device, ¶ 52) configured to allow a user (e.g., person) to select any one of a plurality of accounts (e.g., "Credit Card and other financial information" in FIG. 1) associated with the user to employ in a financial transaction, comprising (Abstract, ¶ 17, 52, FIG. 1, 3-4 with associated text):

- a biometric sensor (e.g., data input devices, such as voice and other audio and video capture devices) configured to receive a biometric input provided by the user (¶ 17, 42);
- a user interface (e.g., user interface **26**) configured to receive:
    - a user input including secret information (e.g., personal identification number) known to the user (¶ 42, 53) and
    - identifying information (e.g., biometric information) concerning an account selected by the user from the plurality of accounts (Abstract, ¶ 43, 47, 57, FIG. 1, 3-4 with associated text);
- a communication interface (e.g., Internet) configured to communicate with a secure registry (e.g., database **24**) (¶ 38, 41); and
- a processor (e.g., CPU **16**) coupled to the biometric sensor to receive information concerning the biometric input (¶ 38-42, 48-53, FIG. 1, 3 with associated text), the user interface and the communication interface,
- the processor being programmed to activate (e.g., obtain access) based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured (¶ 38-42, 51-53; 58-59. From ¶ 52, "the term, 'electronic ID device' will be used generically to refer to any of electronic device that may be used to obtain access to the USR database."):
    - to generate a non-predictable value (e.g., non-predictable single use codes, ¶ 52) and

- to generate encrypted authentication information from the non-predictable value, information derived from at least at a portion the biometric input and the secret information (¶ 12, 45, 51-53, 74, 98, 100. Weiss discloses (1) "transactions to and from the database may take place using a public key/private key security system" from ¶ 12 and (2) "a secret user code and/or time varying value…and personal identification code… combines these three numbers using a predetermined algorithm to generate a one-time nonpredictable code" from ¶ 51 is used to authenticate the user.), and
- to communicate the encrypted authentication information via the communication interface to the secure registry (¶ 12, 45, 51, 100).

Regarding Claim 2, Weiss discloses:

- wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device (¶ 17, 51-52, 74 and FIG. 10, 17 with associated text), and
- wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device (FIG. 8-10 with associated text, see Elements **804**, **904**, **1002**. Observe information flows according to "Merchant transmits to USR".).

Regarding Claim 4, Weiss discloses wherein the device comprises a discrete code associated with the electronic ID device (¶ 74).

Regarding Claim 5, Weiss discloses wherein at least a portion of the biometric received by the biometric sensor is communicated to the secure registry for authentication prior to generation of the encrypted authentication information (¶ 12-13, 16-17, 41-42, 47-48).

Regarding Claim 6, Weiss discloses wherein the secret information includes the identifying Information (¶ 53).

Regarding Claim 13, Weiss discloses wherein the biometric sensor is configured to receive and process *at least one* (Only one option is required to satisfy the claimed limitation of 'at least one') of a fingerprint (e.g., fingerprint), a speech/voice input (e.g., voice print), an iris scan (e.g., iris), a retina scan, a facial scan (e.g., facial), written information (e.g., signature) and a DNA input (e.g., DNA analysis) (¶ 17).

Regarding Claim 14, Weiss discloses:

- wherein the processor is configured to generate account identifying information for the respective one of the plurality of accounts (¶ 51-53),
- wherein the account identifying information does not identify an account number of the respective one of the plurality of accounts (¶ 67-68, 87).

Regarding Claim 15, Weiss discloses a method of generating authentication information comprising acts of (Abstract, ¶ 17, 47-48, 54):

- authenticating an identity of a user to an electronic ID device (e.g., electronic ID device, ¶ 52) based on *at least one* (Only one option is required to satisfy the 'at least one' limitation) of biometric data received by the device from the user and secret information known to the user and provided to the device (¶ 17, 51-53);
- activating (e.g., obtain access) the electronic ID device based on successful authentication (¶ 51-53, 58-59; in particular ¶ 52);
- generating, responsive to activating, a non-predictable value with the device (¶ 51-53, 58, 74);
- receiving, in a user interface (e.g., user interface **26** from FIG. 1), identifying information from the user concerning a selected one of a plurality of user accounts (Abstract, ¶ 74, FIG. 1 with associated text);
- generating encrypted authentication information from the non-predictable value, information derived from at least a portion of the biometric data, and the secret information (¶ 12, 45, 51-53, 74, 98, 100. Weiss discloses (1) "transactions to and from the database may take place using a public key/private key security system" from ¶ 12 and (2) "a secret user code and/or time varying value…and personal identification code… combines these three numbers using a predetermined algorithm to generate a one-time nonpredictable code" from ¶ 51 is used to authenticate the user.); and
- communicating, by a communication interface (e.g., Internet), the encrypted authentication information to a secure registry (e.g., database **24**) (¶ 12, 34, 41, 45, 51, 100).

Regarding Claim 16, Weiss discloses an act of displaying, on the user interface indicators for the plurality of user accounts stored in a memory of the device ("…the verifying section of the database may contain a picture to be transmitted back to the person seeking to validate the device to ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided with a picture of the person authorized to use the card to provide facial confirmation of the person's right to use the card", ¶ 53).

Regarding Claim 17, Weiss discloses de-activating the device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the device (¶ 108).

Regarding Claim 18, Weiss discloses generating a seed from which the authentication information is generated by employing the biometric data and the secret information known to the user (¶ 17, 51-53, 74. Two options satisfy the 'at least two' limitation which are listed by Weiss).

Regarding Claim 19, Weiss discloses generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by a secure registry (FIG. 3, 6-10, 13 with associated text).

Regarding Claim 20, Weiss discloses a method of controlling access to a plurality of accounts, the method comprising acts of (Abstract, ¶ 17, 47-48, 54):

- generating, with a device, encrypted authentication information (¶ 12, 45, 98) from a non- predictable value generated by the device (¶ 51-53),
    - information derived from at least a portion of a biometric of the user received by the device (¶ 17, 51-53) and
    - secret information provided to the device by the user (¶ 17, 53);
- communicating the encrypted authentication information from the device to a secure registry via a point-of-sale (POS) device to authenticate or not authenticate the device with the secure registry (¶ 12, 45, 51-53, 74, 100);
- authorizing the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated (¶ 74-76. ¶ 76 provides the results of a transaction.); and
- denying the POS device from initiation of the financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is not successfully authenticated (¶ 74-76. ¶ 76 provides the results of a transaction.).

Regarding Claim 21, Weiss discloses:

- an act of generating an account identifier (e.g., user's private key) for the selected one of the plurality of user accounts that does not include an account number (¶ 12), and

- wherein the of generating encrypted authentication information includes using the account identifier for the identifying information (¶ 12-13).

Regarding Claim 22, Weiss discloses wherein (from FIG. 1):

- the processor (e.g., CPU **16** from FIG. 1) is configured to display indicators (e.g., person, financial or other information) for the plurality of accounts in the user interface (FIG. 1 with associated text), and
- the user interface (e.g., user interface **26** from FIG. 1) is configured to accept user selection of a respective one of the plurality of accounts (Weiss discloses his invention may be "used to selectively provide personal, financial or other information about a person", ¶ 12 and handles unlimited amount of accounts according to FIG. 1).

Regarding Claim 23, Weiss discloses wherein the user interface is configured to display options for purchase (¶ 53, 99-100. Buyer must authenticate age and identity before purchasing alcohol because alcohol is an age-restricted product. Weiss' invention transmits back "user's photograph, age information" of buyer to merchant's user interface.).

Regarding Claim 24, Weiss discloses wherein the user interface is configured to accept selection of at least one product or service (¶ 53, 99-100. Weiss' invention demonstrates a buyer of legal age will be accepted to buy alcohol.).

Regarding Claim 25, Weiss discloses displaying options for purchase on the user interface (¶ 53, 99-100. Buyer must authenticate age and identity before purchasing alcohol because alcohol is an age-restricted product. Weiss' invention transmits back "user's photograph, age information" of buyer to merchant's user interface.).

Regarding Claim 26, Weiss discloses selecting with the user interface at least one product or service for purchase (¶ 53, 99-100. Weiss' invention demonstrates a buyer of legal age will be accepted to buy alcohol.).

Regarding Claim 27, Weiss discloses displaying options for purchase on the user interface (¶ 53, 99-100. Buyer must authenticate age and identity before purchasing alcohol because alcohol is an age-restricted product. Weiss' invention transmits back "user's photograph, age information" of buyer to merchant's user interface.).

Regarding Claim 28, Weiss discloses selecting with the user interface at least one product or service for purchase (¶ 53, 99-100. Weiss' invention demonstrates a buyer of legal age will be accepted to buy alcohol.).

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss and further in view of US 6819219 ("Bolle") from IDS.

Regarding Claim 7, Weiss discloses a memory coupled to the processor (¶ 17, 52, FIG. 1 with associated text.).

Weiss does not directly disclose wherein the memory stores information employed by the device to authenticate the biometric received by the biometric sensor (¶ 17, 52, FIG. 1 with associated text).

However, Bolle teaches a memory stores information employed by the device to authenticate the biometric received by the biometric sensor (Figure 1, 7 and 10 with associated text. Observe Figure 10, Element 1004). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the devices as disclosed by Weiss by incorporating biometric readers on portable devices as taught by Bolle in order to capture biometric information on a portable device.

9. Claims 8-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss in view of Bolle and further in view of Official Notice (as evidenced by prior art references listed in PTO-892).

Regarding Claim 8, Weiss/Bolle Combination does not directly disclose wherein the device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the device.

The Examiner takes Official Notice it is well known in the art a mismatch or non-matched biometric reading not belonging to the rightful user provides a negative result which prevents access (As evidenced by Drexler (US 5457747), C7:64-C8:27 and FIG. 3 with

associated text.). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the devices as disclosed by Weiss/Bolle Combination by incorporating a measure which prevents access when biometric readings do not match as taught by Official Notice (as evidenced by Drexler) in order to increase security to personal equipment and information.

Regarding Claim 9, Weiss discloses:

- wherein the secret information known to the user includes a PIN (¶ 17, 53), and
- wherein the authentication of both the secret information and the biometric input activate the device for a financial transaction ("The identity of the user possessing the identifying device may be verified at the point of use via *any combination*…", ¶ 17, 73, 100).

Regarding Claim 10, Weiss discloses a memory coupled to the processor (¶ 17, 52, FIG. 1 with associated text.).

Weiss/Bolle Combination does not directly disclose wherein data stored in the memory is unavailable to an individual in possession of the device until the device is activated.

The Examiner takes Official Notice it is well known in the art credit card holders call a telephone number associated with the credit card number to activate their credit cards before they are allowed to make purchases (As evidenced by Flitcroft (US 20030028481) which states, "…when a new credit card is presently issued, it is commonly required that the card holder activate the card. Specifically, the card holder may be required to communicate with the credit

card issuer to activate the card before it can be used", ¶ 200). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the devices as disclosed by Weiss/Bolle Combination by incorporating an activation step as taught by Official Notice (as evidenced by Flitcroft) in order to verify the rightful credit card holder has obtained their card.

Regarding Claim 11, Weiss/Bolle Combination does not directly disclose wherein the data is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the device is activated.

The Examiner takes Official Notice it is well known in the art the credit card data is blocked from making purchases until activated (As evidenced by Flitcroft (US 20030028481) which states, "when a new credit card is presently issued, *it is commonly required that the card holder activate the card*" ¶ 200. Thus the card is not yet active to make any purchase.). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the electronic ID devices as disclosed by Weiss/Bolle Combination by incorporating a protection step of preventing access to credit card usage as taught by Official Notice (as evidenced by Flitcroft) in order to protect the credit card holder in the event the card is obtained by someone other than the intended credit card holder.

Regarding Claim 12, Weiss discloses

- a memory:
    - coupled to the processor (¶ 17, 52, FIG. 1 with associated text) and

- configured to the device (¶ 17, 52, FIG. 1 with associated text),

- wherein the processor is configured to generate a seed using *at least two* (Only two option are required to satisfy the 'at least two' limitation) of the electronic serial number, a discrete code associated with the device (¶ 74), the PIN (¶ 17, 53), a time value (¶ 51), and the biometric input (¶ 17) to generate the encrypted authentication information (¶ 51-53, 74), and
- wherein the seed is employed by the processor to generate the non-predictable value (¶ 51-53, 74).

Weiss/Bolle Combination does not directly disclose store an electronic serial number.

The Examiner takes Official Notice it is well known in the art electronic devices that operate an operating system have unique registration number (As evidenced by Krasinski (US 20030084332) which states, "several unique or distinct identifiers exits" one of which is an "operating system registration number", ¶ 17.). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the devices as disclosed by Weiss/Bolle combination by incorporating a unique digital number as taught by Official Notice (as evidenced by Krasinski) in order to identify the device.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

11. Examiner Calvin Cheung's direct telephone number is (571) 270-7041 and direct fax is (571) 270-8041 and can normally be reached Monday - Friday, 8:00a.m. - 5:00p.m., EST.

If attempts to reach the Examiner are unsuccessful, Primary Patent Examiner Tuan To's telephone number is (571) 272-6985. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CALVIN CHEUNG/

Examiner, Art Unit 3662