



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
61/332,140	05/06/2010	Bjorn Markus Jakobsson	CARBP001+	63419

The entity status change request below filed through Patent Center on 02/13/2023 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Robyn Wagner/	R Wagner	50575



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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/332,140	05/06/2010		110	MJAKP001+		

CONFIRMATION NO. 1008

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



OC000000041793480

Date Mailed: 05/27/2010

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Bjorn Markus Jakobsson, Mountain View, CA;

Power of Attorney:

Robyn Wagner--50575

If Required, Foreign Filing License Granted: 05/25/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/332,140**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

REDUCING FRAUD

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international

page 1 of 3

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Bjorn	Markus	Jakobsson	Mountain View	CA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.**Add****Title of Invention** REDUCING FRAUD

Attorney Docket Number (if applicable) MJAKP001+

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number 21912

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☒ Yes, applicant qualifies for small entity status under 37 CFR 1.27☐ No**Warning**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Robyn Wagner/			Date (YYYY-MM-DD)	2010-05-06
First Name	Robyn	Last Name	Wagner	Registration Number (If appropriate)	50575

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Reducing Fraud

Markus Jakobsson

One type of fraud is committed by a family member, friend, or colleague of a victim. The fraudster may know the password to a financial account of the victim and initiate a payment for some merchandise on behalf of the victim, or may transfer money to themselves from the victim. This can be done using a traditional computer or mobile device, using web-based payments. The fraudster may also have access to the victim's phone, and use this to perform a payment -- e.g., using premium SMS.

These fraudsters are typically not hardened criminals, but regular people who fall for the temptation, maybe thinking that they may eventually pack back the money. They are generally people who would reject pickpocketing as immoral, and who would not take money out of the wallet of the victim. Yet, they feel comfortable initiating fraudulent transactions from accounts they are not the rightful owners of.

Unfortunately, this is a very common type of fraud. While the fraudster can be identified much more often than for other types of fraud, it still results in large losses for service providers. Sometimes, these losses may be due to having to investigate claims, but other times, the service provider may lose the money involved in the fraudulent transaction. For example, consider a situation where a fraudster uses a family member's phone to perform a small payment by premium SMS, and where the account owner notices the charge on the monthly bill and files a complaint with the carrier. The carrier will then typically refund the contested amount without further efforts to resolve the problem (especially since resolving it may be expensive to them!) and will then perform a charge-back to the merchant to whom the payment was made. Even if the merchandise is a digital good, it represents a loss to the merchant. In cases where there is a third party clearinghouse between the carrier and the merchant, this entity may absorb some of the losses.

Using the techniques described herein, losses due to fraud committed by fraudsters close to the victim are reduced. We refer to this type of fraudsters as "friendly fraudsters".

While a friendly fraudster feels comfortable accessing the victim's bill payment account and pay their own bills, or use the victim's phone to pay for some goods or service, he or she would typically not take bills out of the victim's wallet, steal checks and forge the victim's signature, etc. One reason is that this *feels* like a crime, whereas initiating a funds transfer does not to the same extent. Thus, one reason people generally do not steal from friends in part due to a feeling of guilt if they were to.

In various embodiments, a user interface is configured to remind would-be friendly fraudsters of the morality of the actions they are about to perform. This is accomplished without interfering with the normal operations for the legitimate users, and without complicating or delaying their tasks. In short, a feeling of guilt for unwanted behavior is invoked.

A second reason for people to avoid stealing from friends is the risk of getting caught.

In various embodiments, a user interface is configured to remind would-be friendly fraudsters of the risk of being apprehended. This is accomplished by recording contextual information that may help identify the perpetrator to the victim, should the victim be given

access to the recorded information.

In some embodiments an icon representing the legitimate account user is used. For a user with multiple accounts, there may be several icons representing the account user. Furthermore, for a device with multiple users, there may be multiple icons representing users. The icon representing the user may be a photo of the user's face, such as what users often upload to represent themselves for online services with accounts. An icon representing money is also used. This may be an image of a bill, for example. An icon that represents the recipient of a potential payment can also be included. This icon may depend on the actual payee (e.g., be the logo of the payee) or may be a generic icon representing a payee. The embodiment may consist of further components, such as an image representing a hand.

A hand is attached to the face of representing the account owner, and the hand would hold the money-icon. To initiate or complete a payment, the user has to move the money-icon from the hand of the account owner to the icon of the payee. On a touch screen, this may be achieved simply by a sliding motion of the finger. It may also be achieved using a click-and-drag approach, or using another way of indicating the desire to perform the payment, such as a voice command "pay!", or the clicking of a button that says "Pay". As the payment indication is performed, the money icon would move from the account owner icon and the hand icon to the recipient icon, which serves as a reminder to the requester that money is being transferred from the account owner. This makes the transaction more tangible and visual than a transaction that simply involves responding to an SMS, clicking a "submit" button, or similar. The display of money serves to help invoke the notion of cash being moved, and the movement of the money icon away from the account owner icon serves to remind the user that the cash is being transferred. This is all done to mimic a situation in which money is taken from the wallet.

It is possible to have multiple icons representing sources, and multiple icons representing destinations. For example, multiple hands may be used to represent different forms of payments. It is also possible to let all different forms of payments be represented symbolically by one and the same icon, such as an image representing cash. Moreover, multiple destinations may be used to represent different options, such as the speed of shipping and the associated costs. Further icons, such as a gift package icon, can be used to signal a wish to process the order in a particular manner, e.g., gift wrap it. The legitimate account owner, whose image represent the source of the money, would not be notably inconvenienced by this process. Similarly, a person who is asked by the account owner to transfer the funds would probably not be concerned with the visualization of the flow. The visual reminder of the transfer, and the reminder that this transaction moves cash, is likely to make a large portion of would-be friendly fraudsters reconsider the action.

The techniques described herein can be used with devices and services that are not protected by passwords, or where passwords are commonly shared. It can be implemented by web services, such as online payment services. This can be done using JavaScript (or similar technology) to control the display, interaction and movement. It can also be implemented as a browser extension that is installed by a user wishing to remind family members of his or her wish, but who does not want to password protect an account. It may also be dedicated software residing on a mobile or stationary device.

In various embodiments, voice prompts can be used to initiate the transfer of funds or resources. For example, a user can say "yes, please" for a transfer to be performed. This can optionally be recorded. It is also possible that a notification be sent to a pre-specified location (email, voice mail, etc) for some or all of the recorded approvals. This can be done

if the voice profile does not match the profile of previous transactions (e.g., determined by Fast Fourier Transform or other methods of analyzing the input). It is also possible to record and report other types of approval indications, such as the fingerprint (if the device is equipped to read this), photograph of face or hand, or the time and location of the request. It is possible to detect that static images are not photographed, e.g., by taking more than one photo within a short period of time, and determining that there are features suggesting liveness of the photographed object. Requests that meet a pre-specified profile can be further processed and/or reported to the user or other parties. It is possible to flag transactions that are considered anomalous, and not to complete these until they have been investigated. It is also possible to merely record them. Whether the recorded material is used or not, the *possibility* of them being used can be used to increase the feeling among friendly fraudsters that they may be apprehended.

One example process for using the techniques described herein is as follows:

A user uploads or selects a representation of himself or herself, 101. As one example, a camera on a phone could be used to provide the picture. Alternatively, this image assignment could be done by somebody else, or done automatically. In some embodiments the image is taken from another service provider where the user has uploaded a photo or other image. The image 101 may be processed to enhance it or remove unnecessary details, resulting in image 102. This may also involve user-selected additions and distortions, such as medieval helmets, bridal veils, exaggeration of features, etc. There is a collection of images of hands 103, an associated collection of images 104 that also represents a resource, such as money, a key, or other symbol of value or access. An image of a hand is selected from the collection 104, resulting in an image 105. This may be done manually or automatically, and done to match or complement the image 102. In some embodiments this is done as part of the setup of a user account.

When the user's device or account is used to initiate a payment or other access to resources, a combined image 106 is displayed. One can represent a potential payee or recipient of the resource using a corporate logo, a symbol of the recipient, or an image 203 or 204 of a user representing the recipient. As part of completing this transfer of resources, the user would indicate the transfer of the resources from 106 to the selected recipient 203. This could be done by click-and-drag of the resources, by voice command, or by other input. It could also be done automatically as a result of other actions. As this is done, the image 105 is moved to a representation of the recipient, or away from the image 102 component of image 106. Sounds may be played back to match the action, or to otherwise describe the transfer. The selection of sound may depend on the type, size or context of the transaction, or be based on whether the transaction has preliminarily been flagged as anomalous, should that information be readily available at the time a sound is to be selected. Alternatively, the hand associated with 105 may remain static while the representation of resource or access associated with 105 may be moved or removed. Alternatively, a portion of the image of the resource or access representation is removed, resulting in an empty hand. This emphasizes the removal or loss of the resource or access from the person associated with image 102.

It is possible to display multiple potential images 102 that a user can select from to indicate whose resource or access rights will be used. It is also possible to display multiple potential images 203 or 204 to represent multiple recipients of resources or access rights, and select which one will receive these. These selections can be made by drag-and-drop, clicking, voice command, keyboard entry or other indication using a user interface. It could also occur as a result of another action or transaction. The selections can also be made by an application.

The images 101, 102, 103, 104, 105, 106, 203, 204 may be photographic representations, drawings, caricatures, or descriptions, such as a text "Laura's savings" instead of image 102. The recipient image 203 may indicate a value statement of the funds transfer, such as a trash can (for a payment of a category that has been identified as not beneficial), or an image of a purpose like a beach umbrella (symbolizing savings towards a vacation). The selection of these images can be done automatically or manually by the user, according to account types, payment amounts, names of payees, account balances, past purchases, and other contextual information.

The transfer of funds, resources or access may require different types of user commands depending on their size, type, history of other transactions, user preferences, account balances, and other context. For example, it may be that some types may require the click-and-drag of image 105 or parts thereof through a labyrinth; the avoidance of obstructions; the successful participation in a game; or a test of knowledge or skill. Other types may require other actions, such as a basic click on the screen, a voice command "pay", or may be performed automatically. The merchant, payment provider, or other entity may require different actions for different types of payments, different contexts, and different users. For example, a given user may have to say 'Yes, I agree to pay these charges' for one type of transaction, but 'Pay' for another transaction. Instructions of what to say may be provided on the screen, or may be known to the user only. That could provide a type of protection, similar to a password, but which could rely in part on frequency analysis. In the case when it is performed automatically, the transfer of access or resources could still be shown on the screen or other output devices. It may be that the transfers of certain types require the user to make a recorded statement, such as "yes I want to do this"; this recorded statement could be saved, communicated and analyzed to determine whether it matches a given template. The determination whether a given transaction would occur could be made based on the performance of a user of such tests, actions, or in general sequence of inputs.

The context of a transfer request can be saved and exported. This includes voice data, location, web browsing history, photographs, fingerprints, handwritten requests (such as a "yes" written on the screen with the user's finger, or a signature), and other data that potentially could identify a user. The user could be asked to state "I am Bob" (the account owner's name) in order both to record voice and emphasize the misconduct in the case of friendly fraud. The captured data may be analyzed at the time of the transaction, and the success of the transaction be dependent on it; or it can be analyzed in case of a complaint; or in batches some time inbetween, for the sake of potential notification to the account owner. It is possible to require the captured data to conform to some minimal requirement, such as sounding like "I am Bob" (or a handwritten "yes") within some tolerance or threshold.

Another example of the process is described below.

In 303, a hypothetical payment page shown on a smartphone. Since password entry is cumbersome on devices and other constrained devices, many users may opt for a feature allowing them to be recognized. Such features may identify that it is their device, or possibly some context, such as a believable GPS location. Such methods may not have any means of distinguishing between different people, which may encourage friendly fraud.

In 304, another checkout is shown. Many people choose to always be signed in for some services, such as those provided by Google. Whereas this is convenient, it may also encourage friendly fraud.

306 shows a login page. In many cases, users set their browsers to remember and autofill passwords, in which case anybody with access to the computer can perform this step.

Images 301 and 302 show different checkouts. It may be that a user does not have to enter a password in order to complete the transaction, as shown in 303, 304 and 306. Alternatively, passwords may be used in the checkout process. This process may correspond to a sequence, such as what is shown in 305, 306, 307 and 308. This corresponds to the sequence of webpages a user typically may see when performing a purchase.

To improve this traditional checkout process, a webpage showing an image 106 representing ownership may be shown as part of this process. To proceed past this step, the user would have to indicate movement of the resource 105. The resulting sequence may be 305, 106, 306, 307, 308. Alternatively, one may remove the step 306, corresponding to what was shown in 303. The step corresponding to 106 may be part of one of the other actions. For example, it may be that it is part of 305, and that the visual transfer of resources corresponding to 106 is done instead of clicking "proceed to checkout", or other instead of "Buy now with 1-click." Similarly, it can be made part of 306. That is shown in 309, which is a combination of 306 and 106. In that example, which suggest a voice-driven login, the user has to say "Pay" to make the representation of funds be moved to the icon representing the payee, following the red arrow. For another user, the image would be different, and would represent that user. If no user image is available, a generic image can be used, and the user asked to upload an image of himself/herself. Another example is shown in 310, which is a combination of 302 and 106, where the transfer is committed to by the user photographic his/her face. The application may contain basic face-detecting techniques to make sure that a face is actually photographed. It may also contain functionality to make sure that it is not a photo, e.g., require minor changes between two snapshots taken with a very short delay between as the user presses the button to photograph.

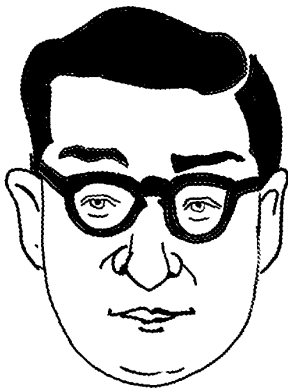
The step corresponding to 106 can be iterated for different webpages in the checkout flow, e.g., both as part of 305 and 307. The step corresponding to 106 can be used consistently instead of or in addition to any button that indicates agreement to proceed with the transaction.

It is also possible to add 106 before or after 301, 302, 303, or 304, or make them part of these webpages.

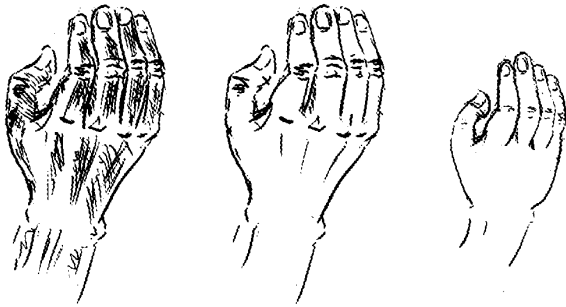
Drawings



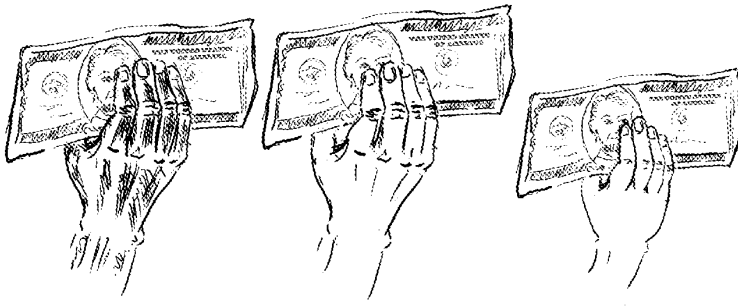
101. A representation of a user



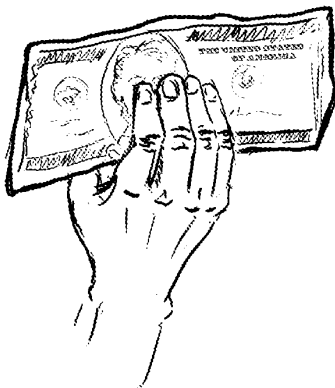
102. Background removed from user's photo, and photo potentially enhanced.



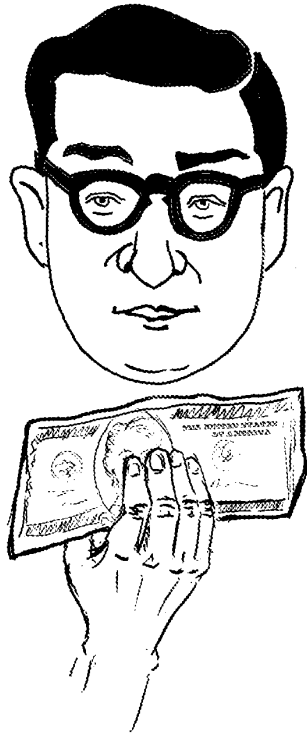
103. Different pre-loaded images of hands. A hand is selected, either manually or automatically, to match the face 102.



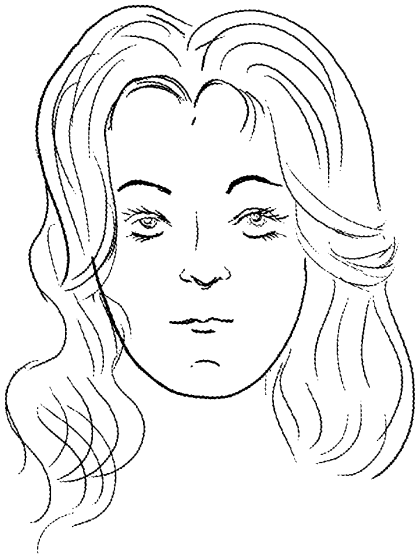
104. Different pre-loaded images of hands with added representations of resources, such as money.



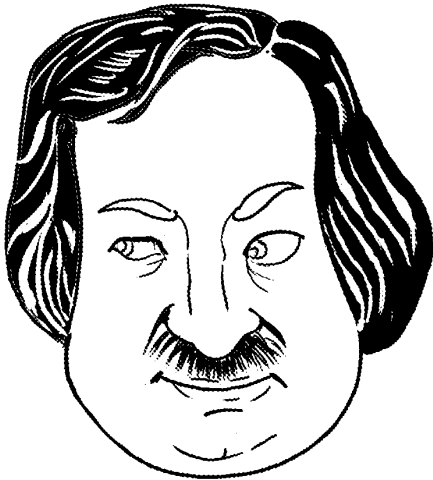
105. A selection of a hand with resource 104.



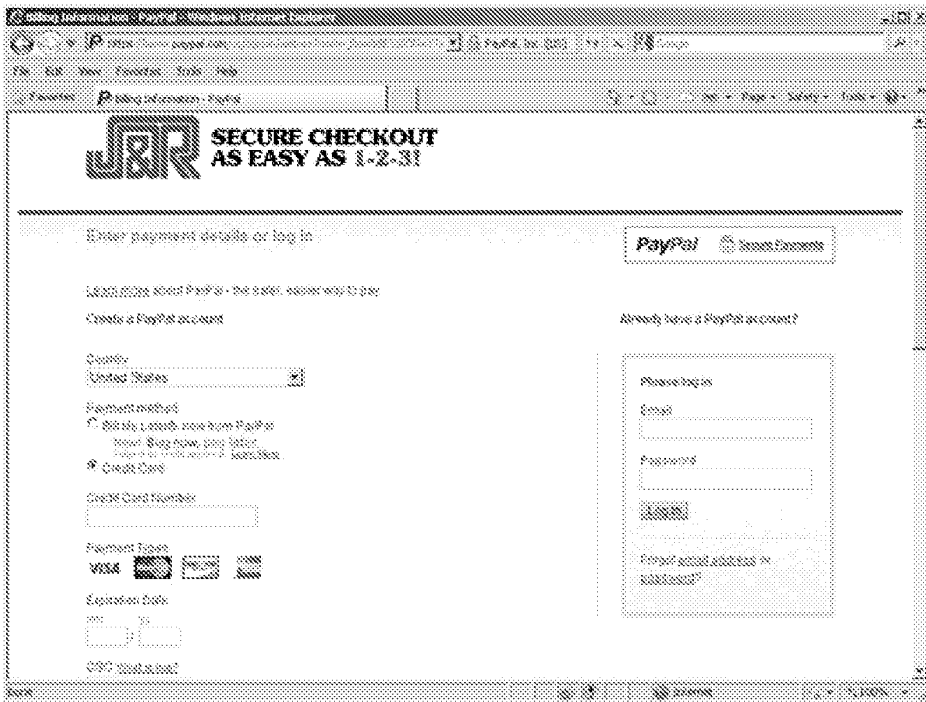
106. The combination of 102, a selected hand with an image representing a resource 105.



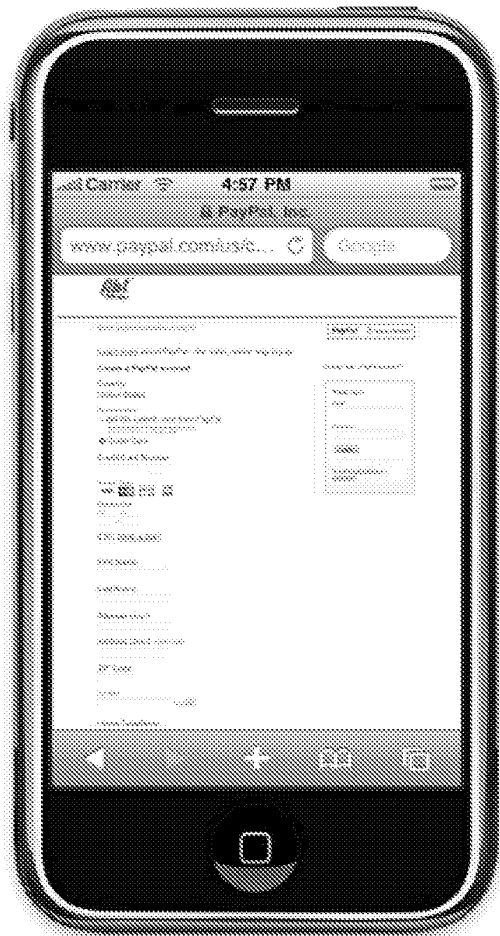
203. An alternative user.



204. A second alternative user.



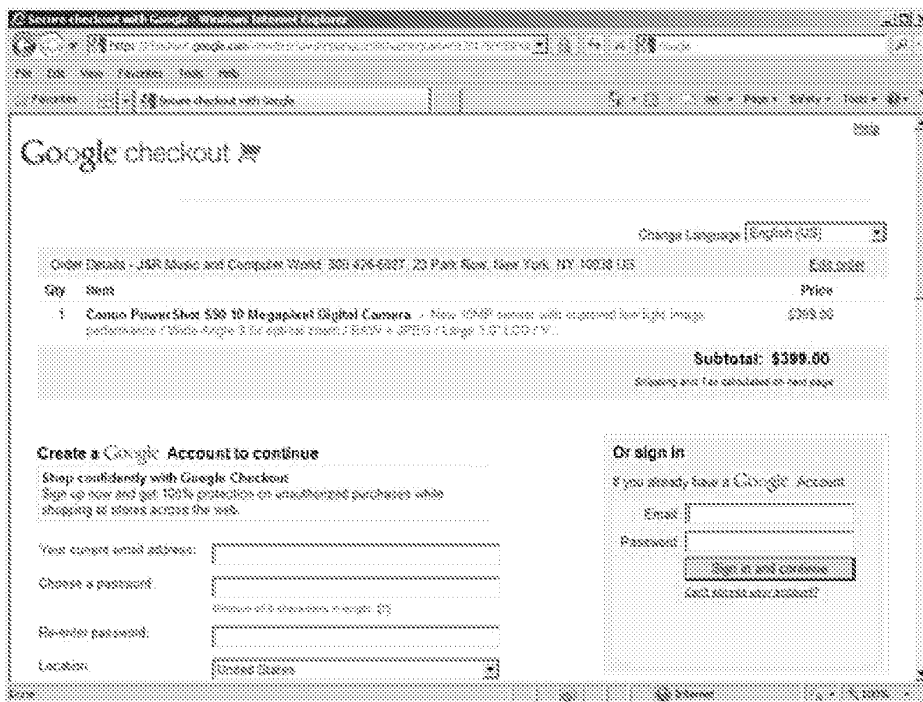
301. A webpage showing a checkout.



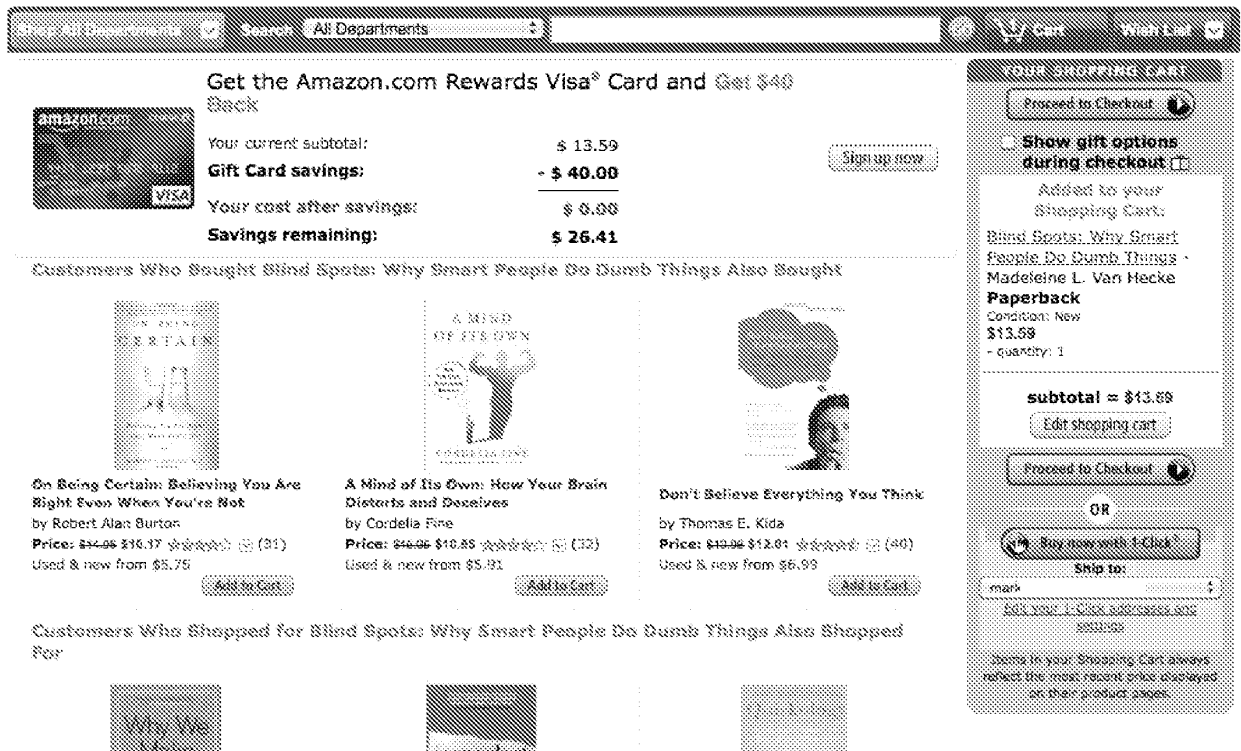
302. A phone displaying a payment webpage.



303. An example display during the checkout process.



304. An example checkout screen.



305. A webpage showing a pending purchase.

amazon.com



0

[SIGN IN](#) [REGISTER & PURCHASE](#) [GIFT WRAP](#) [PLACE ORDER](#)

Ordering from Amazon.com is quick and easy

Enter your e-mail address:

☐

I am a new customer.
(You'll create a password later)

☐

**I am a returning customer,
and my password is:**



[Forgot your password? Click here](#)

[Has your e-mail address changed since your last order?](#)

Redeeming a gift card or gift certificate? We'll ask for your claim code when it's time to pay.
Having difficulties? Please visit our [Help](#) pages to learn more about placing an order.

[Conditions of Use](#) [Privacy Notice](#) © 1996-2009, Amazon.com, Inc.

306. A webpage showing the login step.

Review the information below, then click "Place your order."

Place your order

Shipping to: [Change](#)

markus.jakobsson

Shipping Options: [Learn more](#)

Choose your ~~Prime~~ shipping speed:

☐ FREE Standard Shipping (3-5 business days)

☒ **FREE Two-Day Shipping** --get it Friday, May 7!

☐ \$3.99/item One-Day Shipping --get it tomorrow Thursday, May 6!

Need to [Change quantities or delete](#)?

Estimated delivery date for this item: May 7, 2010 -- Friday

Blind Spots: Why Smart People Do Dumb Things - Madeleine L. Van Hecke

\$13.59 - Quantity: 1 - In Stock - Amazon Prime: Two-Day Shipping is free

Condition: New

Sold by: Amazon.com, LLC

☐ **Gift options** None [Change](#)

Order Summary

Amazon Prime Member

Items:	\$13.59
Shipping & Handling:	\$0.00
Total Before Tax:	\$13.59
Estimated Tax:	\$0.00
Order Total: \$13.59	

Amazon Prime Shipping has been applied to the eligible items in your order.

Have any gift cards, gift certificates or promotional claim codes? [Learn more](#)

Enter them here (one at a time):

[Apply](#)

Payment Method:

[Change](#)

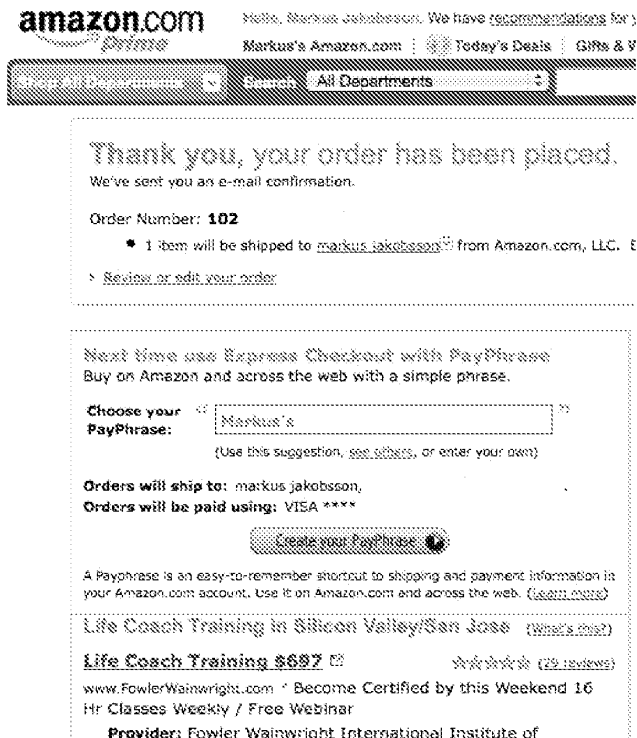
Visa : ***

Exp:

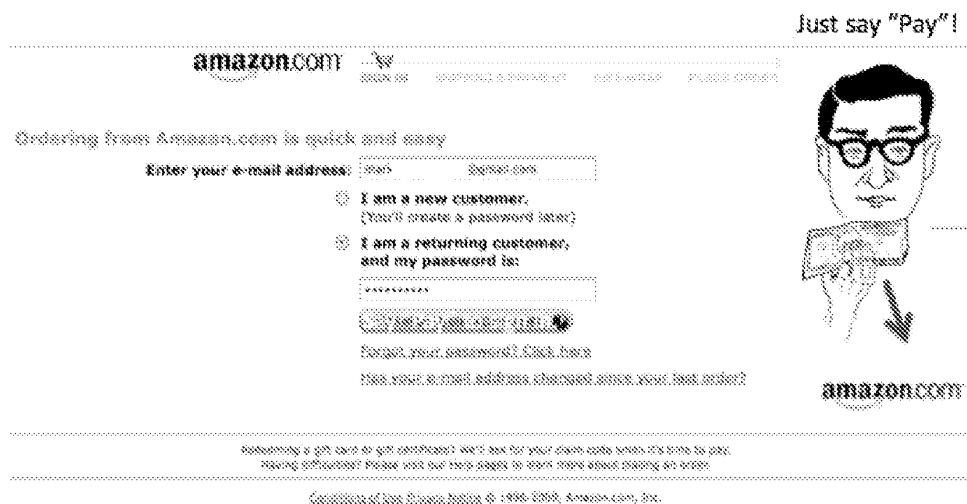
Billing Address: [Change](#)

markus.jakobsson

307. A webpage showing the purchase to be made.



308. A webpage showing a conformation of a purchase having been made.



309. An augmented webpage.

MJACP001+

16



310. An augmented checkout.

The techniques described herein can be used to communicate two different messages to two different types of users. Namely, to the legitimate user, the user interface communicates "you are now paying", while to a friendly fraudster, it communicates "you are now stealing - and to add to that, from your friend!".

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		REDUCING FRAUD		
First Named Inventor/Applicant Name:		Bjorn Markus Jakobsson		
Filer:		Robyn Erinn Wagner/Veronica Pula		
Attorney Docket Number:		MJAKP001+		
Filed as Small Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional Application filing fee	2005	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				110

Electronic Acknowledgement Receipt	
EFS ID:	7567484
Application Number:	61332140
International Application Number:	
Confirmation Number:	1008
Title of Invention:	REDUCING FRAUD
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Robyn Erinn Wagner/Veronica Pula
Filer Authorized By:	Robyn Erinn Wagner
Attorney Docket Number:	MJAKP001+
Receipt Date:	06-MAY-2010
Filing Date:	
Time Stamp:	19:22:26
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$110
RAM confirmation Number	4672
Deposit Account	500685
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	MJAKPP001plus_Provisional_Coversheet_Efile.pdf	1000070 270eaf865076007dd4a879bc1b0f67088cef1b03	no	3
Warnings:					
Information:					
2	Specification	MJAKP001plus_Application.pdf	2325719 51f664bd2e16ca4ec52a52461b408bc18cd014ea	no	17
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	29542 57badb9d00397e7e26c3145b94223a6cf96c2237	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			3355331		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. New Applications Under 35 U.S.C. 111 If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. National Stage of an International Application under 35 U.S.C. 371 If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. New International Application Filed with the USPTO as a Receiving Office If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					