(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 463 477**

(51) Int. CI.:

H04K 1/00 (2006.01)
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04M 1/66 (2006.01)
H04M 1/68 (2006.01)
H04M 3/16 (2006.01)
H04M 11/00 (2006.01)
G06F 21/31 (2013.01)
G06F 21/42 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.12.2000 E 00988057 (6)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2014 EP 1238336**

(54) Título: **Sistema de red dual y método para autenticación o autorización en línea**

(30) Prioridad:

15.12.1999 US 170808 P
13.12.2000 US 737254

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.05.2014

(73) Titular/es:

AUTHENTIFY, INC. (100.0%)
8745 West Higgins Road, Suite 240
Chicago, IL 60631, US

(72) Inventor/es:

WOODHILL, JAMES R.

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema de red dual y método para autenticación o autorización en línea

Campo de la Invención

Esta invención se relaciona de manera general con la seguridad en Internet. Más particularmente, esta invención se relaciona con el método para tratar de verificar la identidad de un usuario de Internet.

Antecedentes de la Invención

La Internet ofrece la posibilidad de comercio mundial expandido, comercio electrónico, con potencialmente menor costo para los compradores de lo que era posible hasta ahora. Sin embargo, la falta de contacto directo de persona a persona ha creado su propia serie de problemas. El robo de identidad es un problema que amenaza el crecimiento del comercio electrónico.

El crecimiento del comercio electrónico sólo se producirá si existe una infraestructura de seguridad confiable y verdadera en el lugar. Es imperativo que se verifique la identidad de los visitantes del sitio antes de otorgarles acceso a cualquier aplicación en línea que requiere confianza y seguridad. De acuerdo con el Centro Nacional de Fraude, su estudio del robo de identidad “lo lleva a la inevitable conclusión de que la única solución de sentido amplio realista para el robo de identidad es a través de autenticación”. Identity Theft: Authentication As A Solution, página 10, nationalfraud.com.

Con el fin de “autenticar” una entidad, se debe:

1) identificar a la entidad como una entidad “conocida”,

2) verificar que la identidad que se afirma por la entidad es su verdadera identidad, y

3) proporcionar un rastro de auditoría, que conmemora las razones para confiar en la identidad de la entidad.

En el mundo físico, gran parte de la seguridad percibida de los sistemas se basa en la presencia física. Tradicionalmente, con el fin de abrir una cuenta bancaria, el solicitante debe aparecer físicamente en una sucursal bancaria, afirmar la identidad, llenar formularios, proporcionar firmas en tarjetas de firma, etc. Es habitual que el banco a petición del solicitante, proporcione una o más formas de identificación. Esta es la forma en que el banco verifica la identidad afirmada del solicitante. Si el banco, por ejemplo, acepta una licencia de conducción como una forma de identificación, entonces el banco realmente se basa en la integridad del procesamiento de los sistemas de la agencia estatal que expide la licencia de conducción de que el solicitante es quien ha afirmado ser.

El rastro de auditoría que el banco mantiene incluye todos los formularios que se pueden haber completado (que incluyen tarjetas de firmas), copias de documentos importantes (tales como licencia de conducción), y tal vez una foto tomada con propósitos de identificación. Este proceso destaca la confianza que se tiene en un proceso de identificación y autenticación verdadero en presencia física.

En el mundo electrónico, el escenario sería muy diferente. Un solicitante aparecería en el sitio web de registro del banco, ingresa la información afirmando una identidad y hace clic en un botón para continuar el proceso. Con este tipo de registro, el único rastro de auditoría, que el banco tendría es que una entidad de una determinada dirección IP aparece en el sitio web e ingresa determinada información. La entidad puede de hecho haber sido un dispositivo automatizado. La dirección IP que inicia la transacción es probablemente una dirección asignada dinámicamente que se emite a partir de un grupo de direcciones disponibles. En resumen, el banco realmente no tiene la garantía de identidad verdadera de la entidad que registra la cuenta.

Para resolver este problema, muchos proveedores de sitios de comercio electrónico han empezado a contar con mecanismos que no se producen como parte de la transacción electrónica real para ayudar a proporcionar garantía de que la transacción es auténtica. Estos mecanismos se denominan generalmente como mecanismos de “fuera de banda”. El mecanismo de autenticación fuera de banda utilizado con más frecuencia es enviar al usuario final un fragmento de correspondencia a través del Servicio Postal de los Estados Unidos u otros servicios de distribución similares. El fragmento de correspondencia enviado al usuario final contendrá algún fragmento de información que el sitio requiere que el usuario final posea antes de proceder con el registro.

Al enviar algo (por ejemplo, un número de PIN) a través del correo, y luego solicitar que el usuario final utilice ese fragmento de información para “continuar” en el sitio web, el proveedor del sitio se basa en los efectos de disuasión de ser forzado a recibir un fragmento de correspondencia en un lugar, que incluye, pero no se limita a, las leyes federales que están destinadas a prevenir el fraude electrónico. El principal inconveniente de utilizar el correo es que es lento. Adicionalmente, no existe ningún rastro de auditoría. En esta época de la Internet, esperar “7 a 10 días” para que un paquete de correo llegue no es ideal para el consumidor o el sitio de comercio electrónico.

El documento DE19718103A1 describe un sistema que envía una contraseña a un usuario a través de una ruta de transmisión, tal como un teléfono celular, que es diferente a aquella utilizada por el dispositivo de entrada empleado para contactar el sistema, cuya contraseña luego se introduce en el dispositivo de entrada.

Un factor de autenticación es algo que se puede utilizar para verificar que alguien es quien él o ella dice ser. Los factores de autenticación generalmente se agrupan en tres categorías generales: algo que sabe, algo que tiene, y algo que es.

Un “algo que sabe” es un fragmento de información que solo, o tomado en combinación con otros fragmentos de información, debe ser conocido sólo por la entidad en cuestión o aquellos en quien la entidad en cuestión debe confiar. Los ejemplos son una contraseña, el nombre de soltera de la madre, número de cuenta, PIN, etc. Este tipo de factor de autenticación también se denomina como un “secreto compartido”.

Un secreto compartido sólo es efectivo si se mantiene en forma confidencial. Desafortunadamente, los secretos compartidos son a menudo demasiado fáciles de determinar. En primer lugar, el secreto compartido a menudo se deriva demasiado de la información que está relativamente ampliamente disponible (Número de Seguro Social, número de cuenta). En segundo lugar, es difícil para un ser humano mantener un secreto que alguien también realmente quiere. Si alguien realmente quiere información suya, puede hacer un gran esfuerzo para conseguirla, ya sea preguntándole o preguntando a los que le rodean, directa o indirectamente, o al determinar la información de otros que puedan conocerlo.

Un “algo que tiene” es cualquier token físico que apoya la premisa de una identidad de la entidad. Ejemplos son claves, tarjetas con banda magnética y tarjetas inteligentes. Los tokens físicos de manera general, requieren algún mecanismo fuera de banda para suministrar realmente el token. Usualmente, es necesario algún tipo de presencia física (por ejemplo, un empleado que aparece en la oficina de recursos humanos para recoger y firmar por las llaves del edificio).

Los tokens físicos proporcionan el beneficio agregado de no ser “capaces de ser diseñados por ingeniería social”, lo que significa que sin el token físico, cualquier cantidad de información conocida por una parte de mala reputación no sirve de nada sin el token. Una parte de confianza debe producir el token de una forma confiable.

Un “algo que es” es alguna característica de una persona que se puede medir y utilizar para identificar de manera única un individuo dentro de una población. Ejemplos son huellas dactilares, retina, tono de voz. Las capacidades biométricas ofrecen la mayor forma de autenticación de identidad disponible. Requieren algún tipo de presencia física y son capaces de representar características únicas de una persona que son extremadamente difíciles de falsificar.

Por ejemplo, el documento EP 0 444 351 A2 describe un sistema de seguridad controlado con contraseña de voz, en el que un ordenador instituye una llamada de voz a un teléfono asociado con un usuario. El ordenador solicita al usuario repetir una serie seleccionada de forma aleatoria de dígitos o una frase que consiste en un grupo de palabras. El ordenador luego compara la información de voz recibida en la línea de voz con la información de voz prealmacenada asociada con el supuesto usuario. El ordenador proporciona acceso a sus recursos si y sólo si se produce una coincidencia de voz.

Infortunadamente, los dispositivos biométricos aún no son totalmente confiables, y el hardware para respaldar los dispositivos biométricos es caro y aún no se despliega ampliamente. Alguna tecnología biométrica en uso hoy en día también se basa en una “imagen” electrónica de los valores biométricos con los que se compara. Si esta imagen electrónica alguna vez se compromete, entonces el uso de esos valores biométricos como identidad se ve comprometido. Esto se convierte en un problema serio basado en el número limitado de valores biométricos disponibles en la actualidad. Más importante, no se pueden utilizar valores biométricos para determinar la identidad de un individuo en el primer caso.

Una infraestructura de seguridad es sólo tan fuerte como su modelo de confianza subyacente. Por ejemplo, una infraestructura de seguridad basada en credenciales de seguridad solo puede superar los problemas de fraude y robo de identidad si inicialmente se distribuyen credenciales de seguridad a las personas correctas.

Por lo tanto, el registro por primera vez, y la emisión inicial de credenciales de seguridad, son la clave de cualquier infraestructura de seguridad; sin una herramienta confiable para verificar inicialmente la identidad, una infraestructura de seguridad falla completamente. El Centro Nacional de Fraude señaló explícitamente este problema en la página 9 de su informe:

> "Existen varios niveles de seguridad utilizados para proteger la identidad de los propietarios [credenciales de seguridad]. Sin embargo, la limitación de seguridad conocida es el proceso utilizado para determinar que la persona que obtiene la [credencial de seguridad] es realmente esa persona. Los únicos medios conocidos para realizar esta determinación es a través del proceso de autenticación".

En cualquier modelo de seguridad, la distribución de credenciales de seguridad enfrenta el mismo problema: cómo verificar la identidad de la persona a través de la Internet anónima. Se presentan tres métodos conocidos para intentar verificar la identidad de un visitante del sitio. Los tres métodos actuales se resumen adelante:

- Solución A: una organización requiere la presencia física de un usuario para autenticación. Mientras el usuario está presente, se puede recolectar valores biométricos físicos para uso posterior (huella dactilar, muestra de voz, etc.). El problema con el modelo de presencia física es que es muy difícil y costoso para una compañía requerir que todos sus empleados, socios y clientes se presenten físicamente con el fin de recibir una credencial de seguridad electrónica. Este modelo se vuelve más difícil y más costoso a medida que aumenta a un gran número de usuarios.

- Solución B: una compañía identifica y autentica a un individuo con base en un secreto compartido que las dos partes han acordado previamente. El problema con el modelo secreto compartido es que en sí mismo crea un serio problema de seguridad: se pueden comprometer fácilmente los secretos compartidos. Dado que el secreto compartido es relativamente fácil de obtener, este modelo de seguridad sufre de graves índices de fraude. El uso de una copia electrónica de un valor biométrico específico como una huella digital se podría utilizar como un secreto compartido. Pero una vez esté comprometido, no se puede volver a emitir una nueva huella digital y existe un número limitado de otras para elegir.

- Solución C: una compañía se basa en la comunicación de un secreto compartido a través del servicio postal. Este proceso inicia cuando el usuario se registra en un sitio web e ingresa información que lo identifica únicamente. Luego se envía un número de identificación personal (PIN) al usuario a una dirección de correo postal (suponiendo que la información de identificación es correcta). El usuario debe recibir el PIN en el correo, vuelve a la página web y se registra de nuevo para introducir el PIN. Se utiliza el servicio postal, porque es una red de confianza; existe cierta garantía de entrega a la parte esperada y hay implicaciones legales en caso de incumplimiento de la red. Un gran defecto de este método es el retraso incorporado de días, incluso semanas, antes de que el usuario reciba el PIN. Este modo de autenticación es demasiado lento para los estándares de negocios de hoy en día; el potencial de Internet para transformar la estructura del comercio se apoya firmemente en la capacidad de procesar las transacciones rápidamente. Demasiadas personas simplemente nunca terminan el proceso. Más aún, se presenta un rastro de auditoría limitado para referirse a, en el caso de una disputa con respecto al uso de la credencial de seguridad. Se podría requerir una firma (otro tipo de valor biométrico), pero que triplica el retraso hasta que se devuelve el PIN. Las organizaciones están viendo que gran número de clientes potenciales no regresan para cerrar una transacción después de estos retrasos.

La Tabla I resume las características de los procesos de autenticación conocidos.

Tabla I

	Procesos de autenticación		
Características	Presencia física	Correo	Secretos compartidos
Automatizado			✓
Fácilmente escalable		✓	✓
Auditable	✓	✓	
Puede utilizar valores biométricos	✓		

(continuación)

	Procesos de autenticación		
Características	Presencia física	Correo	Secretos compartidos
Tiene protecciones legales	✓	✓	
Ocurre en tiempo real, por lo tanto tiende a retener clientes			✓
Disuade de fraude	✓	✓	
Protege los datos privados	✓		

Las soluciones conocidas no permiten a las organizaciones distribuir de manera eficiente y segura las credenciales de seguridad electrónicas. Continúa subsistiendo la necesidad de métodos de autenticación o autorización mejorados. Preferiblemente, se podrían realizar dichas mejoras sin crear complejidad adicional sustancial para un visitante de un sitio. También sería preferible si dichos métodos no ralentizan el ritmo de la interacción o transacción.

Resumen de la Invención

De acuerdo con la presente invención se proporciona un sistema de red dual para emitir credenciales de seguridad que comprende: un primer sistema que consiste de un sistema de comunicación de red telefónica conmutada pública, y un segundo sistema, que es una red electrónica distinta del primer sistema, por lo menos en parte; un teléfono acoplado al primer sistema; una terminal de usuario acoplada al segundo sistema; un sitio objetivo, en comunicación con la terminal de usuario a través del segundo sistema cuando se ha conectado un visitante del sitio en la terminal de usuario al sitio objetivo a través de un navegador de Internet que corre en la terminal de usuario, el sitio objetivo que se dispone para llevar a cabo una transacción a solicitud del visitante en la terminal de usuario; y un servidor de autenticación/autorización dispuesto para ejecutar instrucciones para comunicarse con el visitante en la terminal de usuario a través del segundo sistema; en donde: el sitio objetivo se puede operar para solicitar que el visitante proporcione información de identificación, para confirmar un número telefónico con el visitante en el que se pueda ubicar al visitante, para proporcionar al servidor el número telefónico confirmado, y dirigir al visitante al servidor; el servidor se puede operar para que visualice una página web y ejecute instrucciones para colocar una llamada, a través del primer sistema, al número telefónico proporcionado del visitante, para remitir información de confirmación a la terminal de usuario del visitante, a través del segundo sistema, y solicitar, a través del primer sistema, que el visitante hable o teclee la información de confirmación, visualizada en la terminal de usuario, que puede indicar el contrato para los términos y condiciones de la transacción, comparar la información de confirmación remitida con la información de confirmación recibida, y determinar si es la misma, devolver una respuesta al sitio objetivo, y redirigir al visitante al sitio objetivo; y el sitio objetivo se puede operar para determinar si el visitante ha cumplido los requerimientos de la transacción, y, si es así, emitir una credencial de seguridad electrónica al visitante a través del segundo sistema.

Un sistema automatizado utiliza una red de comunicaciones disponible públicamente, tal como la Red Telefónica Conmutada Pública (PSTN), línea cableada o inalámbrica, para proporcionar un mecanismo en tiempo real, interactivo y principalmente de auto-servicio para ayudar en la autenticación (verificaciones de identidad) y autorización (aceptación mediante una identidad verificada) para transacciones electrónicas. Se coordinan las acciones entre una red electrónica (la Internet) y la Red Telefónica Conmutada Pública.

Se puede utilizar esta coordinación de una sesión activa de Internet con una sesión de PSTN activa como una herramienta para verificación. Se puede utilizar para crear un rastro de auditoría para cualquier transacción electrónica individual. Estas transacciones pueden ser, por ejemplo, la primera emisión de tiempo de una credencial de seguridad electrónica (por ejemplo, contraseñas, certificados digitales, PIN) o la verificación de una credencial de seguridad ya emitida. Otras transacciones, sin limitación, vienen dentro del alcance de la presente invención tal como se define en las reivindicaciones.

A un visitante que ha iniciado la sesión en un sitio para obtener productos, servicios, credenciales, acceso o similares, todo sin limitación, se le solicita ingresar o especificar un número telefónico donde él/ella pueda ser contactado durante la sesión actual (entorno de múltiples líneas), o entre segmentos de la presente sesión (entorno de única línea). El software de autenticación/autorización puede en este momento transmitir información de

confirmación específica a la pantalla del usuario. Esta información está solo disponible para el software de transmisión y el receptor.

El software de autenticación/autorización luego realiza una llamada, a través de la Red Telefónica Conmutada Pública, al visitante del sitio. Se solicita al visitante del sitio, al recibir la llamada desde el software, que teclee a través del teclado del teléfono o lea de nuevo la información de confirmación a través de la red telefónica. Se entenderá que se puede variar el orden y el tiempo de presentación y captura de información de confirmación con base en la solicitud.

Esta confirmación “fuera de banda” tiene la ventaja de que la información de confirmación se suministra al visitante inmediatamente, mientras que está en línea. En un entorno de múltiples líneas, el visitante permanece en línea y recibe una llamada telefónica automatizada, al número telefónico identificado esencialmente inmediatamente. El visitante proporciona retroalimentación inmediata de la información de confirmación, con el software.

Adicionalmente a la información de confirmación, el software puede iniciar un intercambio basado en voz, con el usuario. Este intercambio se puede almacenar para proporcionar un rastro de auditoría. El mismo rastro de auditoría puede incluir el número telefónico llamado, la información de confirmación no verbal y/o cualquier información adicional relacionada con la transacción.

Una vez el software ha autenticado o autorizado al visitante, se puede transferir al visitante, con autorización o indicios de acceso apropiados al software que proporciona transacción o acceso.

La coordinación de una sesión activa de Internet con una sesión activa de PSTN permite la implementación de un método para proporcionar autenticación de dos factores en tiempo real, totalmente automatizada de un usuario de Internet. Esta invención es una mejora sobre el proceso conocido para ayudar a verificar la identidad de un usuario de Internet. La invención tiene beneficios, ilustrados en la Tabla II, en comparación con los procesos conocidos:

Tabla II

	Procesos de autenticación			
Características	Teléfono	Presencia física	Correo	Secretos compartidos
Automatizado	✓			✓
Fácilmente escalable	✓		✓	✓
Auditable	✓	✓	✓	
Puede utilizar valores biométricos	✓	✓		
Tiene protecciones legales	✓	✓	✓	
Ocurre en tiempo real, por lo tanto tiende a retener clientes	✓			✓
Disuade de fraude	✓	✓	✓	
Protege los datos privados	✓	✓		

El presente método se puede utilizar en relación con:

- registro y emisión de Credenciales de Seguridad Electrónicas (ESC)
- autorización en tiempo real de transacciones sensibles (por ejemplo, alto valor financiero, material sensible a la edad, etc.)
- recolección de información de pago (por ejemplo, información de tarjeta de crédito).

El presente método y sistema cumple un número significativo de requerimientos necesarios para el registro por primera vez efectivo y posterior mantenimiento de credenciales de seguridad: velocidad, seguridad, escalabilidad y un fuerte rastro de auditoría. En un aspecto, se proporciona una herramienta de auto-servicio, automatizada para ayudar a verificar de forma rápida y confiable la identidad de la persona en la Internet.

En otro aspecto, la Red Telefónica Conmutada Pública (PSTN) es un factor en la autenticación. El sistema contiene mecanismos que permiten la sincronización de una sesión establecida sobre una red electrónica, tal como la Internet, con una sesión establecida sobre la Red Telefónica Conmutada Pública (una llamada telefónica).

La capacidad de una persona para responder a una llamada telefónica a su propio número telefónico se comporta como un “algo que tiene” más que un “algo que sabe”. En el caso de un número telefónico, es fácil para una parte de mala reputación determinar su número telefónico (como un algo que sabe), pero es mucho más difícil para la parte de mala reputación obtener realmente acceso a su teléfono para recibir una llamada en el teléfono (como un algo que tiene).

No existe ley en contra de conocer su número telefónico (incluso si no se enumera), pero existen leyes contra el acceso no autorizado a la línea telefónica que su número telefónico representa. El conocimiento del criminal de su número telefónico le permite llamarlo, pero no puede responderle. El sistema actual requiere el uso simultáneo o sustancialmente simultáneo del teléfono y un ordenador cercano conectado a Internet.

Adicionalmente al utilizar la PSTN como un factor de autenticación, el uso de la PSTN también hace posible utilizar una grabación de voz para crear un rastro de auditoría. También se podría utilizar esa grabación de voz como entrada para la biometría de voz (el propio tono voz es un “algo que tiene”) como un factor de autenticación adicional. Esto sería especialmente útil si se debe volver a emitir una credencial de seguridad electrónica para un sujeto que viaja (es decir, fuera de un número telefónico conocido).

En otro aspecto, el sistema se configura de tal manera que el propietario de un sitio puede solicitar cualquier número de grabaciones de voz, entradas de teclado y páginas web para crear una aplicación de autenticación personalizada. Un componente de secuencias de comandos del sistema proporciona esta flexibilidad dentro de las diversas aplicaciones que se ejecutan en el sistema.

La capacidad de las secuencias de comandos permite que se valide una transacción dada en una forma distinta. Por ejemplo, un tipo de transacción sólo podría requerir que se haga una llamada telefónica y que se ingrese un número de confirmación. Otro tipo de transacción puede requerir cuatro grabaciones de voz junto con una entrada de teclado del año en que nació el visitante del sitio.

Se puede crear un registro de transacciones de una sesión de autenticación. El registro de la transacción puede incluir como información de ejemplo, información del visitante del sitio, el propietario del sitio quien envía la solicitud, la grabación de aceptación, la grabación del nombre, la dirección IP del visitante del sitio, el número de confirmación emitido e ingresado, el número telefónico de llamado, un timbre de fecha/hora verdadero, y una firma digital de la información.

El registro de la transacción proporciona un rastro probatorio sustancial de que el visitante del sitio es quien lleva a cabo la transacción de autenticación/ autorización. También se puede utilizar este rastro de auditoría para permitir la terminación de transacciones futuras, en el caso de registro, de re-emisión de credencial de seguridad electrónica con base en los valores biométricos de tono de voz, o percepción equivalente a la Atención al Cliente humana para la grabación de auditoría y compararlo con la voz del visitante del sitio en el teléfono.

Se puede dejar este rastro de auditoría registrado a disposición de los propietarios del sitio a través del teléfono o de Internet (utilizando técnicas tales como audio en tiempo real o reproductores de archivos de audio). También se puede colocar el rastro de auditoría en un servidor que permite al propietario del sitio recuperar los datos a su propia discreción.

Se entenderá que la comunicación entre un sitio de destino y un servicio de autenticación/autorización puede tener lugar de varias maneras. En una forma, el servicio de autenticación puede aceptar una redirección desde el sitio objetivo y tomar el control de la sesión de red con el visitante del sitio. Alternativamente, el sitio objetivo puede mantener el control de la sesión de red con el visitante y comunicarse con el servicio de autenticación/autorización a través de una sesión de red independiente y separada.

Otras numerosas ventajas y características de la presente invención serán fácilmente evidentes de la siguiente descripción detallada de la invención y las realizaciones de la misma, de las reivindicaciones y de los dibujos adjuntos en los que se describen total y completamente los detalles de la invención como parte de esta especificación.

Breve Descripción de los Dibujos

La Figura 1 es un diagrama de bloques de un sistema de acuerdo con la presente invención;

La Figura 2 es un diagrama que ilustra las etapas de un método de acuerdo con la presente invención;

La Figura 3 es un diagrama de bloques del sistema de la Figura 1 para implementar un proceso de registro;

La Figura 4 es una copia de una pantalla del visitante exhibida para iniciar un proceso de registro;

La Figura 5 es una vista de una pantalla de solicitud del visitante para presentar información;

La Figura 6 es una vista de una pantalla del visitante para presentar o seleccionar un número telefónico;

La Figura 7 es una copia de una pantalla del visitante que pregunta al visitante sobre su capacidad para responder una llamada telefónica de forma simultánea mientras que se conecta a Internet;

La Figura 8 es una reconfirmación de la información proporcionada en la pantalla de la Figura 7;

La Figura 9 es una copia de una pantalla del visitante que informa al visitante que se le va a realizar una llamada automatizada mientras que está en línea;

La Figura 10 es una vista de una pantalla del visitante que lleva al visitante a escuchar un mensaje audible presentado a través del teléfono;

La Figura 11 es una pantalla del visitante que ilustra una etapa final del proceso de registro;

La Figura 12 es una pantalla del visitante que reconfirma que el visitante debe desconectarse antes de responder una llamada telefónica;

La Figura 13 es una pantalla que presenta información de confirmación al visitante con instrucciones;

La Figura 14 es una pantalla del visitante que ilustra instrucciones para proceder después que ha concluido la llamada telefónica;

La Figura 15 es una pantalla que solicita que el visitante especifique cuánto tiempo necesita para cerrar la sesión de Internet;

La Figura 16 es una reconfirmación de la información de confirmación presentada previamente en la Figura 13; y

La Figura 17 es una pantalla de cierre de sesión antes de que se realice la llamada telefónica al visitante.

Descripción Detallada de la Invención

Aunque esta invención es susceptible de realización en muchas formas diferentes, se muestra en los dibujos y se describirá aquí en detalle, las realizaciones específicas de las mismas con el entendimiento de que la presente descripción se va a considerar como un ejemplo de los principios de la invención y no se pretende que limite la invención a las realizaciones específicas ilustradas

La Figura 1 ilustra un sistema 10 para llevar a cabo un proceso de autenticación/ autorización, interactivo. En un aspecto, se puede implementar el sistema 10 como se discute adelante utilizando un método de múltiples líneas. Alternativamente, se puede utilizar un método de única línea

El sistema 10 incluye una pantalla del visitante del sitio 12 y ordenador local asociado 14. El visitante del sitio V, a través de un enlace de comunicación bidireccional 16 puede tener acceso, enviar solicitudes a y recibir servicios de un proveedor de servicios de internet 20. El proveedor de servicios de internet 20 que se acoplaría a través de enlaces de comunicación bidireccional 22 se comunica a través de una red electrónica 26, que puede ser la internet disponible públicamente o una intranet privada con un sitio objetivo 30 a través de un enlace de comunicación bidireccional 32.

En una transacción típica, el visitante V inicia sesión en el sitio objetivo 30 y solicita, autorización, autenticación u otros servicios solos o en combinación desde el sitio 30. En respuesta a una o más solicitudes del visitante V, el sitio

30, a través de un enlace de comunicación bidireccional 34 y la red 26 se comunican a través de otro enlace 36 con un servidor de autenticación/ autorización 38.

El servidor 38 incluye software de autorización/autenticación en la forma de instrucciones ejecutables prealmacenadas P. También incluye bases de datos D en donde se almacena información en relación con transacciones previas, o, información proporcionada previamente suministrada por el sitio objetivo 30.

El servidor de autenticación/autorización 38 hace posible autenticar o autorizar al visitante del sitio V de acuerdo con la presente invención. El servidor 38 recibe ya sea desde el sitio objetivo 30 o directamente del visitante V un número telefónico donde se puede llamar al visitante V o contactarlo esencial e inmediatamente.

El servidor 38 incluye instrucciones ejecutables P para implementar ya sea un entorno de múltiples líneas en donde el visitante V se puede comunicar por el teléfono de forma simultánea mientras que está en línea con el servidor 38 o un entorno de única línea en donde el visitante V debe cerrar la sesión de tal manera que reciba la llamada telefónica discutida posteriormente y luego de nuevo vuelva a iniciar sesión.

En un entorno de múltiples líneas, el servidor 38 interactúa en tiempo real con el visitante V a través de la red 26 y a través de la red telefónica conmutada 44. En esta circunstancia, antes de la llamada telefónica, el software de autenticación/autorización P transmite, a través de la red 26, información de confirmación. Esta información aparece en la pantalla del visitante 12.

La información de confirmación puede incluir secuencias alfanuméricas de información de un tipo, que el visitante V puede teclear en o hablar audiblemente en un teléfono 46. El servidor 38 automáticamente luego realiza una llamada telefónica a través de la red 44 al teléfono 46 utilizando el número suministrado por el visitante del sitio V.

El servidor 38 puede, una vez que el visitante V haya descolgado el teléfono 46, confirmar verbalmente con el visitante V que es de hecho el individuo quien ha iniciado la sesión en el sitio 30 y de hecho ese individuo espera una llamada en ese teléfono. El servidor 38 luego solicita verbalmente que el visitante V teclee o hable de la información de confirmación que solo ha recibido en la pantalla 12.

El servidor 38 también puede solicitar que el visitante V hable en el teléfono 46 para propósitos de crear uno o más archivos de voz almacenados utilizables como parte de un rastro de auditoría.

Asumiendo que se ha retroalimentado la información de confirmación apropiada por el visitante V al servidor 38 utilizando la red 44, el servidor 38 puede dirigir al visitante V para finalizar la llamada telefónica. El servidor 38 luego puede comparar la información de confirmación recibida con la confirmación de transmisión y determinar si son la misma. El control del navegador del visitante luego se puede devolver al sitio objetivo 30 junto con un mensaje que confirma la identificación del visitante V o proporcionar información de autorización en relación con una transacción con base en la información inicial almacenada en la base de datos D del servidor 38. Ya sea uno solo o ambos servidores 38 y el sitio 30 pueden estar involucrados en realizar la decisión de autenticación/ autorización. Luego el sitio 30 continúa la transacción y se comunica directamente con un visitante V.

Se entenderá que se puede transmitir una variedad de tipos de información de confirmación a través del servidor 38 al visitante V utilizando el enlace de transmisión de fuera de banda, a saber la Red Telefónica Conmutada Pública 44. De forma similar, una variedad de respuestas por el visitante V al servidor 38 se puede reenviar al sitio 30, si se desea, para ser utilizadas con el fin de tomar la decisión de autenticación/ autorización.

La Figura 2 ilustra las etapas de un proceso 100 implementado por el sistema 10. El visitante del sitio inicia el proceso de registro en el sitio objetivo 30. En una etapa 102, el visitante V inicia sesión en el sitio objetivo 30 y en una etapa 104 registra en la página de registro existente en el sitio objetivo, al proporcionar información de identificación preliminar. En una etapa 106, el sitio 30 confirma un número telefónico con el visitante V en el que se puede contactar inmediatamente al visitante. Por ejemplo, el sitio objetivo podría preguntar al visitante si un número telefónico almacenado en sus registros de visitante del sitio es correcto o preguntar al visitante por el tipo en un número telefónico. El proceso luego se transporta temporalmente a un servidor de autenticación/autorización 38. Es decir, el sitio 30 luego se redirige al visitante junto con el número telefónico del visitante al servidor 38.

En una etapa 108, el servidor 38 asume el control del navegador del visitante e inquiere del visitante si puede realizar una llamada en ese número telefónico mientras que el visitante está en línea, en un entorno de múltiples líneas, cuando el usuario responde “si”, la sesión en línea continúa con el servidor 38 que reenvía un código de confirmación a través de la red 26 que es a su vez presentada en la pantalla 12. Si el visitante responde “No”, el servidor: exhibe un número de confirmación en la pantalla, así como también el URL de una página web “Finaliza Registro”, dice al visitante que tome nota del número de confirmación y el URL, y luego da instrucciones al visitante para desconectarse de Internet.

En una etapa 110, el servidor 38 realiza una llamada telefónica al número telefónico proporcionado a través de la red 44 que debe producir que timbre el teléfono 46 que a su vez es descolgado por el visitante V. El servidor 38 luego puede confirmar que el visitante V, el destinatario de la llamada, está a la espera de la misma. El servidor 38 luego solicita que el visitante V ya sea hable o teclee la información de confirmación en la pantalla 12.

Adicionalmente para analizar la retroalimentación de información de confirmación a través de la red 44, el servidor 38 en una etapa 112 puede solicitar que el visitante realice declaraciones de voz predeterminadas, de tal manera que el servidor pueda realizar una o más grabaciones digitales de voz. En una implementación estándar la llamada automatizada podría solicitar hasta dos grabaciones de voz distintas, tal como que el visitante recite su nombre, y luego recite un contrato para los términos de una transacción procesada.

Los visitantes quienes permanecen en línea durante la llamada luego pueden colgar el teléfono y terminar la conversación. A los visitantes quienes se han desconectado para propósitos de realizar la llamada telefónica a través de la red 44 se les recuerda iniciar de nuevo la sesión en el sitio 30 y completar la etapa de registro 104.

El servidor 38 luego devuelve el control del navegador del visitante en una etapa 114 al sitio 30. El sitio 30 luego utilizando su software interno determina si el visitante V ha cumplido los requerimientos necesarios para permitir que la transacción continúe. Por ejemplo, el sitio objetivo puede recibir una respuesta desde el servidor que describe la sesión de teléfono automatizada y, con base en los códigos de éxito o falla en la respuesta del servidor, decide si el visitante ha cumplido los requerimientos para registro.

La siguiente discusión y las figuras asociadas ilustran el flujo donde el servidor 38 ayuda al sitio que emite la credencial 30’ en el registro del visitante V, véase Figura 3.

En el siguiente escenario, el visitante del sitio V es un individuo quien ha iniciado sesión en el sitio 30’ para solicitar la credencial de seguridad electrónica. “ESC” significa la credencial de seguridad electrónica. La “solicitud SO” se refiere al software de solicitud que corre en la instalación del “Propietario del Sitio” 30’.

En las siguientes tablas, las etapas enumeradas en la columna más a la izquierda que contienen números en NEGRITA y SUBRAYADO se refieren a interacciones en el servidor 38’. Las etapas que no están en negrita se refieren a interacciones que el visitante del sitio V tiene en el sistema del propietario del sitio 30’.

Las Figuras 4-17 ilustran las pantallas del navegador de Internet de ejemplo, asociadas que se referencian dentro de la columna de Sesión de Internet de la Tabla 3.

Se representan dos escenarios en las Tablas III y IV. La Tabla III marcada “Sincronización Inmediata” se refiere a una sesión donde el visitante del sitio V tiene una conexión de Internet que no interfiere con la llamada telefónica automatizada discutida anteriormente. La Tabla IV marcada con “Sincronización Retrasada” se refiere al visitante del sitio V que utiliza la misma línea telefónica para la conexión de Internet ya que se va a utilizar para recibir la llamada telefónica de autenticación.

Sincronización Inmediata - Tabla III

La Sincronización Inmediata ocurre cuando el visitante V está utilizando un enlace de comunicaciones diferente para la conexión de Internet que se utiliza para la llamada automatizada desde el servidor 38, Figura 1 o 38’, Figura 3.

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
1	El visitante del sitio V llega a un sitio web prescrito 30’ para iniciar el proceso de registro. (Figura 4)		
2	El visitante del sitio ingresa la información en la solicitud del Propietario del Sitio (SO) que se requiere por la página web y presenta la información. (Figura 5)		La información que se va a recolectar se prescribirá por el emisor del ESC, y para propósitos de ejemplo puede contener información de identificación tal como nombre, dirección, número de seguro social, número de empleado, número de cuenta, nombre de soltera de la madre, etc.

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
3	La solicitud SO utiliza la información presentada por el visitante del sitio para consultar un almacén de datos y determinar si la información proporcionada por el visitante del sitio identifica una entidad a la que se va a emitir un ESC por el sistema. (Figura 5)		Se puede validar la información recolectada del visitante del sitio, se revisa por inconsistencias, y se asocia con una identidad existente dentro del sistema de SO.
4	En una realización, la solicitud SO exhibe una lista de ubicaciones de los números telefónicos mantenidos en el almacén de datos para solo la entidad identificada. Esta lista se puede procesar como los nombres de ubicación, el número telefónico completo, o un número enmascarado (555-555-***5), y presentado de nuevo al visitante del sitio en una página web. La página web pide al visitante del sitio identificar en cuál de las ubicaciones enumeradas se puede encontrar al visitante del sitio en ese momento. Se presentan otras varias alternativas que el emisor de una credencial puede seleccionar. Estas incluyen: • Se pueden presentar números telefónicos reales (en lugar de los nombres de la ubicación) • Se le puede pedir al visitante del sitio que ingrese un número telefónico. Se puede utilizar una combinación del nombre de la ubicación y los últimos cuatro dígitos del número para incrementar la exactitud mientras que se mantiene la privacidad. (Figura 6)		
5	El visitante del sitio identifica el número del teléfono en el que se ha contactado él/ella, ya sea al seleccionar un número o nombre de ubicación representativo. Luego se presenta esta información. (Figura 6)		Esta información se presenta al sistema de Registro, el servidor 38'. Por lo tanto, después que el visitante del sitio selecciona un número y hace clic en enviar, él/ella se redirige al servidor de Registro 38'. El visitante del sitio no sabrá de esta transferencia porque las páginas web serán similares a la solicitud SO

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
6	El Servidor 38' presenta una página web que pregunta al visitante del sitio acerca de su capacidad para responder una llamada realizada a un determinado número mientras que se conecta a Internet. La pregunta de ejemplo es "¿Puede llamar al 555-555-***5 mientras que está conectado a Internet?" (Figura 7)		Esta pregunta se presenta al visitante del sitio con el fin de determinar si el visitante del sitio puede recibir la llamada telefónica automatizada mientras que está conectado a Internet. Alternativamente, tienen que desconectar su ordenador con el fin de recibir una llamada telefónica.
7	El Servidor 38' luego presenta una página web al visitante del sitio que reconfirma la decisión que hace él/ella sobre la página previa. Si el visitante del sitio responde "SI" a la pregunta anterior entonces aparecería en pantalla el siguiente texto. "Puedo responder personalmente a las llamadas realizadas al 555-555-***5 al mismo tiempo que mi ordenador está conectado a Internet y puede leer la información exhibida en la pantalla de mi ordenador mientras que utiliza el teléfono" (Figura 8)		Esta página web permite que el visitante del sitio confirme que él/ella puede recibir una llamada telefónica mientras que se conecta a Internet. También permite que el visitante del sitio vuelva a la pregunta previa si la declaración que se presenta a él/ella es incorrecta.
8	El servidor 38' exhibe una página web que dice al visitante del sitio que se le va a realizar una llamada automatizada. La página web también contiene un número de confirmación o cadena alfanumérica (Información de confirmación). (Figura 9)	Se realiza la llamada telefónica automatizada al número prescrito que se le ha solicitado al visitante del sitio,	En este punto, el Servidor 38' empleará una técnica de manejo de estado que permitirá que la sesión de Internet activa sea coordinada con la Sesión PSTN (llamada telefónica). Se deben de manejar de forma apropiada las condiciones de (señal de ocupado, conmutador, etc.). El manejo "Apropiado" dependerá de los requerimientos del propietario de la credencial. Ejemplos son: • Si la línea está ocupada, falla • Si la línea está ocupada, vuelva a intentar después de la pausa

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
9	Se exhibe alguna página web como en la etapa 8. (Figura 9)	Una vez se conteste, el Servidor 38' responderá con un saludo de identificación tal como: "Hola, esta es la llamada telefónica automatizada de la Corporación XYZ. Si usted está esperando esta llamada, presione la tecla numeral. De otra forma por favor cuelgue".	El contenido actual del saludo se puede controlar por el sitio 30' o el Servidor 38' o ambos sin limitación. El servidor 38' puede, como una opción, requerir una acción positiva para que la persona que contesta el teléfono reconozca una identidad. Durante la Sesión PSTN, el Servidor 38' proporcionará al visitante del sitio la capacidad de recibir ayuda en cualquier momento. Si el visitante del sitio presiona la tecla ayuda (tecla * en el teléfono), el sistema reaccionará por los requerimientos del propietario del sitio.
10	Se exhibe la misma página web como en la etapa 8. (Figura 9)	El Servidor 38' dará instrucciones al visitante del sitio para ingresar el número de confirmación de la página web en el teléfono: "Por favor ingrese el número de confirmación visualizado en la pantalla de su ordenador utilizando el teclado del teléfono, luego presione la tecla numeral".	Una vez el visitante del sitio ha ingresado el número de confirmación de la página web en el teléfono. El servidor 38' espera que el que está utilizando el navegador web sea la misma persona que está en la llamada telefónica. El servidor 38' permitirá que el visitante del sitio vuelva a reintentar muchas veces el número de confirmación. El propietario del sitio determina cuántas veces permitirá al visitante del sitio ingresar el número de confirmación.
11	Cuando el visitante del sitio presione la tecla numeral, la página web cambia y tiene el siguiente texto: "Por favor escuche cuidadosamente las indicaciones de las voz del teléfono" (Figura 10)	El Servidor 38' dará instrucciones al visitante del sitio para registrar su nombre: "Para propósitos de auditoría necesitamos registrar su nombre. Después del tono, por favor diga su nombre completo, luego presione la tecla numeral".	El servidor 38' realizará una grabación del nombre para información de rastro de auditoría. El propietario del sitio 30' puede determinar qué información se debe registrar del visitante del sitio V. El servidor 38' permitirá muchas grabaciones o ninguna grabación como lo solicite el propietario del sitio. Una característica de secuencias de comandos proporciona dicha flexibilidad. El servidor 38' tiene mecanismos que aseguran que las grabaciones son de buena calidad. El servidor 38' es capaz de detectar si una voz no es lo suficientemente fuerte o lo suficientemente larga para conseguir una grabación exacta. El servidor 38' puede utilizar estas grabaciones al aplicarles la biométrica de voz para posteriores autenticaciones

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
12	La misma página web como en la etapa 11 (Figura 10)	El Servidor 38' dará instrucciones al visitante del sitio para registrar su aceptación de los términos y condiciones: "La corporación XYZ ahora necesita su aceptación de los términos y condiciones de su sitio web. Después del tono, por favor diga 'Acepto las condiciones', luego presione la tecla numeral".	De nuevo, esta grabación está destinada para ser utilizada como un mecanismo de rastro de auditoría. El propietario del sitio 30' puede determinar si desearía esta grabación de voz o cualesquier grabaciones adicionales. El propietario del sitio 30' decide si el servidor 38' debe utilizar reconocimiento de voz para verificar la aceptación apropiada o utilizar una entrada numérica (por ejemplo "Presione 1 si acepta, 2 si no acepta") como una alternativa.
13	El visitante del sitio se redirige de nuevo a la solicitud del sitio 30' (Figura 10)	El servidor 38' lee un reconocimiento de éxito al visitante del sitio: "Felicitaciones, ha completado su autenticación. Su nuevo usuario y clave se exhiben en la pantalla de su ordenador. Adiós".	Después que el visitante del sitio ha finalizado el procesos prescrito por el propietario del sitio 30', él/ella se redirigirá de nuevo al propietario de la solicitud de sitio 30', permitiendo así el propietario del sitio 30' para distribuir el ESC.
14	El propietario del sitio exhibirá en su sistema la siguiente página web en su proceso. Se puede potencialmente proporcionar al visitante del sitio: - identificador de usuario y clave - certificado digital - número de identificación personal - un correo electrónico a una casilla de un correo electrónico (Figura 11)		El propietario del sitio distribuirá el ESC que el visitante del sitio inicialmente estaba buscando cuando él/ella llega a la solicitud SO en la etapa 1.

Sincronización Retrasada - Tabla IV

El escenario de Sincronización Retrasada ocurre cuando el visitante del sitio V está utilizando la misma línea telefónica para su conexión de Internet cuando él/ella la está utilizando para recibir la llamada telefónica automatizada, de esta manera obliga al visitante del sitio a desconectarse temporalmente de la Internet.

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
1	El visitante del sitio llega a un sitio web prescrito 30' para iniciar el proceso de registro. (Figura 4)		
2	El visitante del sitio ingresa la información en la solicitud del Propietario del Sitio que se requiere por la página web y presenta la información. (Figura 5)		La información que se va a recolectar se prescribirá por el emisor del ESC, y puede contener información de identificación tal como nombre, dirección, número de seguro social, número de empleado, número de cuenta, nombre de soltera de la madre, etc.
3	La solicitud SO utiliza la información presentada por el visitante del sitio para consultar un almacén de datos y determinar si la información proporcionada por el visitante del sitio identifica una entidad a la que se va a emitir un ESC por el sistema. (Figura 5)		Se puede validar la información recolectada del visitante del sitio, se revisa por inconsistencias, y se asocia con una identidad existente dentro del sistema de SO.
4	En una realización, la solicitud SO exhibe una lista de ubicaciones de los números telefónicos mantenidos en el almacén de datos para solo la entidad identificada. Esta lista se puede procesar como los nombres de ubicación, el número telefónico completo, o un número enmascarado (555-555-***5), y presentado de nuevo al visitante del sitio en una página web. La página web pide al visitante del sitio identificar en cuál de las ubicaciones enumeradas se puede encontrar al visitante del sitio en ese momento. Se presentan otras varias alternativas que el emisor de una credencial puede seleccionar. Estas incluyen: • Se pueden presentar números telefónicos reales (en lugar de los nombres de la ubicación) • Se le puede pedir al visitante del sitio que ingrese un número telefónico. Se puede utilizar una combinación del nombre de la ubicación y los últimos cuatro dígitos del número para incrementar la exactitud mientras que se mantiene la privacidad. (Figura 6)		

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
5	El visitante del sitio identifica el número del teléfono en el que se ha contactado él/ella, ya sea al seleccionar un número o nombre de ubicación representativo. Luego se presenta esta información. (Figura 6)		IMPORTANTE Esta información se presenta al sistema. Por lo tanto, después que el visitante del sitio selecciona un número y hace clic en enviar, él/ella se redirige al servidor 38'. El visitante del sitio no sabrá de esto porque las páginas web serán similares a la solicitud SO
6	El Servidor 38' presenta una página web que pregunta al visitante del sitio acerca de su capacidad para responder una llamada realizada a un determinado número mientras que se conecta a Internet. La pregunta de ejemplo es "¿Puede usted llamar al 555-555-***5 mientras que está conectado a Internet?" (Figura 7)		Esta pregunta se presenta al visitante del sitio con el fin de determinar si el visitante del sitio puede recibir la llamada telefónica automatizada mientras que está conectado a Internet. Alternativamente, tienen que desconectar su ordenador con el fin de recibir una llamada telefónica.
7	El Servidor 38' luego presenta una página web al visitante del sitio que reconfirma la decisión que hace él/ella sobre la página previa. Si el visitante del sitio responde "NO" a la pregunta anterior entonces aparecería en pantalla el siguiente texto. "Para responder personalmente a las llamadas realizadas al 555-555-***5 debe primero desconectar mi ordenador de la internet" (Figura 12)		Esta página web permite que el visitante del sitio confirme que él/ella puede desconectar el ordenador de la Internet con el fin de recibir la llamada telefónica. También permite que el visitante del sitio vuelva a la pregunta previa si la declaración que se presenta a él/ella es incorrecta.
8	El servidor 38' presenta una página con una confirmación del número. (Figura 13)		El visitante del sitio necesita escribir o imprimir la página web con el fin de utilizar el número de confirmación durante la llamada telefónica.
9	El servidor 38' presenta una página web que contiene un URL 'www.finishregistration.com'. (Figura 14)		El visitante del sitio necesita recordar o anotar la dirección URL porque después de la llamada telefónica, él/ella necesitará volver a conectarse a Internet y dirigir su navegador web a la dirección URL que se muestra en la página web. La razón para hacer esto es porque el sistema debe cerrar la sesión de los visitantes del sitio antes de redirigir al visitante del sitio a la solicitud SO
10	El servidor 38' luego presenta una página web que permite al visitante seleccionar cómo desean esperar antes de que se les realice la llamada (Figura 15)		El visitante podrá elegir el tiempo de retraso antes de que se haga la llamada telefónica. El SO instruirá en cuanto a los valores que el servidor 38' exhibirá al visitante del sitio.

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
11	El servidor 38' presenta una página web que recuerda al visitante del sitio acerca del número de confirmación y la dirección URL (dirección web) (Figura 16)		El servidor 38' recuerda al visitante del sitio una vez más de las 2 fragmentos de información que necesitará para completar el proceso de autenticación.
12	El servidor 38' presenta una página web que instruye al visitante del sitio desconectarse de la internet y esperar que el sistema realice la llamada telefónica automatizada (Figura 17)		Cuando el visitante del sitio ve esta pantalla el servidor 38' iniciará el temporizador en el retraso de tiempo que se selecciona en la etapa 10. El SO decide si el servidor 38' debe utilizar reconocimiento de voz para verificar la aceptación apropiada o utilizar una entrada numérica (por ejemplo "Presione 1 si acepta, 2 si no acepta") como una alternativa.
13		Inicia la aplicación de voz "Hola, esta es la llamada telefónica automatizada de la Corporación XYZ. Si usted está esperando esta llamada, presione la tecla numeral. De otra forma por favor cuelgue".	Durante la llamada telefónica el visitante del sitio no está conectado a la aplicación web. Este primer mensaje ayuda a identificar que el servidor 38' ha contacto la parte pretendida.
14		"Por favor ingrese su número de confirmación, luego presione la tecla numeral"	Esta etapa le pide al visitante del sitio ingresar el número que se le dio anteriormente sobre la aplicación web. Esto asegura que la persona que estaba en la sesión web es la misma persona que está al teléfono
15		"Para propósitos de auditoría necesitamos registrar su nombre. Después del tono, por favor diga su nombre completo, luego presione la tecla numeral".	Estas etapas toman una grabación de voz del visitante del sitio para propósitos de auditoría. El servidor de 38' puede utilizar estas grabaciones al aplicarles la biometría de voz para autenticaciones posteriores.
16		"La corporación XYZ ahora necesita su aceptación de los términos y condiciones de su sitio web. Después del tono, por favor diga 'Acepto las condiciones', luego presione la tecla numeral".	Esta etapa toma otra grabación de voz del visitante del sitio para propósitos de auditoría. El servidor de 38' puede utilizar estas grabaciones al aplicarles la biometría de voz para autenticaciones posteriores.

(continuación)

Etapa	Sesión de Internet	Sesión PSTN	Comentarios
17		"Felicitaciones, ha completado su autenticación telefónica. Por favor vaya a la dirección de internet www.finishregistration.com para completar su registro. Debe reconectarse dentro de 20 minutos para completar el proceso. Adiós".	Esta es la última etapa de la sesión telefónica. Después de que el visitante del sitio ha completado esta etapa él/ella debe volver a conectar su ordenador a Internet y dirigir su navegador web a 'www.finishregistration.com'. Esto ayuda a reforzar la información que se le da al visitante del sitio en las etapas 9 y 11. El Servidor 38' tiene la capacidad de solicitar a un visitante del sitio que se vuelva a conectar su ordenador y vaya a la dirección Web apropiada dentro de un cierto período de tiempo. La cantidad de tiempo se puede configurar según lo solicitado por el propietario del sitio.
18	El visitante del sitio V vuelve a conectar su ordenador a Internet y se va por ejemplo a: www.finishregistration.com (Fig. 17)		El servidor 38' luego comprueba que los visitantes del sitio están llegando de nuevo a la página web y hace que todos los controles adecuados aseguren que él/ella de hecho ha terminado la sesión telefónica. Si todos los controles son exitosos el visitante del sitio se redirige de nuevo a la solicitud SO en la misma forma exacta que la etapa de escenario de Sincronización Inmediata 13. Permitiendo así que el SO distribuya el ESC
19	El propietario del sitio exhibirá en su sistema la siguiente página web en su proceso. Se puede potencialmente proporcionar al visitante del sitio: - identificador de usuario y clave - certificado digital - número de identificación personal - un correo electrónico a una casilla de un correo electrónico (Figura 11)		El propietario del sitio distribuirá el ESC que el visitante del sitio inicialmente estaba buscando cuando él/ella llega a la solicitud SO en la etapa 1.

La siguiente es una lista de condiciones de error de muestra que pueden ocurrir y una sugerencia de cómo se pueden manejar. El manejo de muchas de estas condiciones es en gran medida una cuestión de política que va a decidir el propietario del sitio 30'. Cada uno de estos casos de falla tiene como una posible respuesta que no se pudo completar el registro electrónico

Tabla V

	Condición de Error	Posible respuesta
1	señal de ocupado	• Espere 30 segundos y vuelva a llamar. • Presente las instrucciones en la web para elegir un número diferente o despeje la línea.
2	Llamada telefónica alcanza conmutador	• Presente grabación actual solictanfo transferencia a los visitantes del sitio. • Transfiera al agente humano en el lado de iniciación de la llamada, solicite transferencia al visitante del sitio, transfiera de regreso a la operadora automática. • Reproduzca los tonos DTMF de la extensión del sistema al que está tratando de llegar
4	El visitante del sitio cancelan la sesión web	La Sesión PSTN les da las gracias por participar y termina la llamada.
5	El visitante del sitio cancela la sesión PSTN	La Sesión Web presenta la página que ofrece mecanismos alternativos de registro.
6	No hay captura de grabación de voz	• Proporcionar instrucciones para hablar en voz más alta. • Registro de Falla • No acepta inscripción con ninguna auditoría de voz

De lo anterior, se observará que se pueden efectuar numerosas variaciones y modificaciones sin apartarse del alcance de la invención como se define en las reivindicaciones. Es de entenderse que no se pretende ni se debe inferir ninguna limitación con respecto a la realización específica ilustrada aquí. Se pretende que la descripción cubra las reivindicaciones adjuntas, todas dichas modificaciones que caen dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un sistema de red dual (10') para emitir credenciales de seguridad que comprende:

un primer sistema (44) que consiste de un sistema de comunicación de red telefónica conmutada pública (44), y un segundo sistema (26), que es una red electrónica distinta del primer sistema (44), por lo menos en parte;

un teléfono (46) acoplado al primer sistema (44);

una terminal de usuario (12, 14) acoplada al segundo sistema (26);

un sitio objetivo (30'), en comunicación con la terminal de usuario (12, 14) a través del segundo sistema (26) cuando un visitante del sitio en la terminal de usuario (12, 14) se ha conectado al sitio objetivo (30') a través de un navegador de Internet que corre en la terminal de usuario (12, 14), el sitio objetivo que se dispone para llevar a cabo una transacción a solicitud del visitante en la terminal de usuario (12, 14); y

un servidor de autenticación/autorización (38') dispuesto para ejecutar instrucciones para comunicarse con el visitante en la terminal de usuario (12, 14) a través del segundo sistema (26);

en donde:

el sitio objetivo (30') se puede operar para solicitar que el visitante proporcione información de identificación, para confirmar un número telefónico con el visitante en el que se pueda ubicar al visitante, proporcionar al servidor (38') el número telefónico confirmado, y dirigir al visitante al servidor (38');

el servidor (38') se puede operar para que visualice una página web y ejecute instrucciones para hacer una llamada, a través del primer sistema (44), al número telefónico proporcionado del visitante, para remitir información de confirmación a la terminal de usuario (12, 14) del visitante, a través del segundo sistema (26), y para solicitar, a través del primer sistema (44), que el visitante hable o teclee la información de confirmación, visualizada en la terminal de usuario (12, 14), para comparar la información de confirmación remitida con la información de confirmación recibida, y determinar si son las mismas, para devolver una respuesta al sitio objetivo (30'), y para volver a dirigir al visitante al sitio objetivo (30'); y

el sitio objetivo (30') se puede operar para determinar si el visitante ha cumplido los requerimientos de la transacción, y, si es así, emitir una credencial de seguridad electrónica al visitante a través del segundo sistema (26).

2. Un sistema como en la reivindicación 1 en donde el segundo sistema (26) comprende un sistema telefónico conmutado con una porción inalámbrica.

3. Un sistema como en la reivindicación 2 en donde el enlace de comunicaciones del segundo sistema (26) se establece de forma simultánea con otro enlace de comunicaciones utilizando el primer sistema (44).

4. Un sistema como en la reivindicación 1, 2 o 3, en donde el servidor (38') se puede operar adicionalmente para solicitar que el visitante registre un contrato para los términos y condiciones de la transacción.

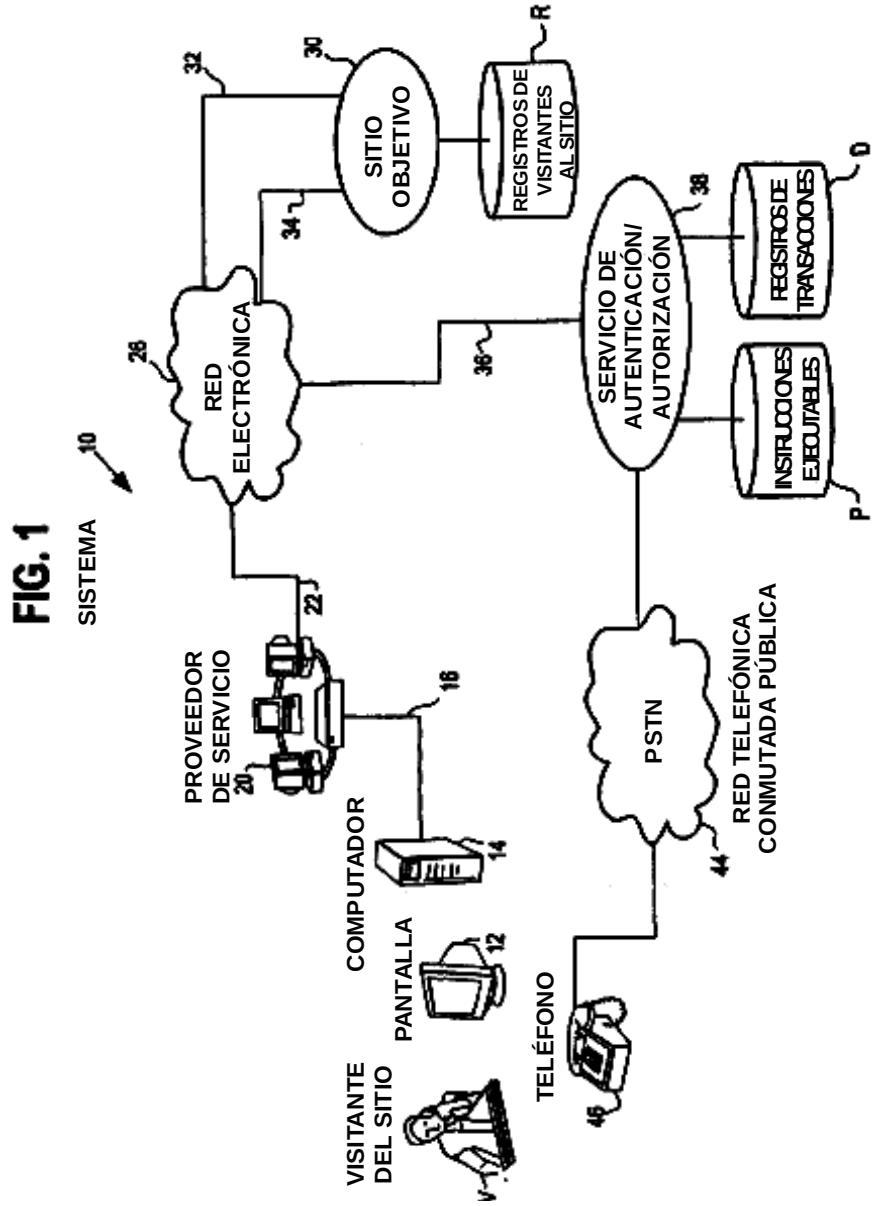


FIG. 1
SISTEMA
10
RED ELECTRÓNICA
26
SITIO OBJETIVO
30
REGISTROS DE VISITANTES AL SITIO
R
SERVICIO DE AUTENTICACIÓN/ AUTORIZACIÓN
38
REGISTROS DE TRANSACCIONES
D
INSTRUCCIONES EJECUTABLES
P
PROVEEDOR DE SERVICIO
20
COMPUTADOR
14
PANTALLA
12
VISITANTE DEL SITIO
V
TELÉFONO
46
PSTN
44
RED TELEFÓNICA CONMUTADA PÚBLICA
32
34
36
22
16

FIG. 2A

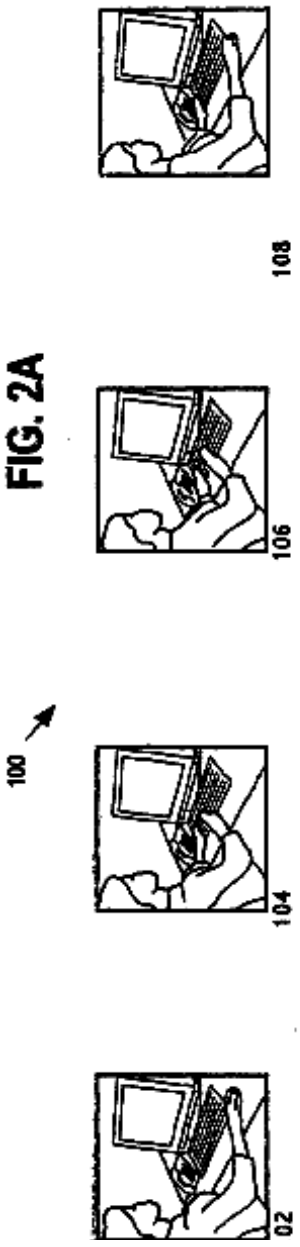


FIG. 2

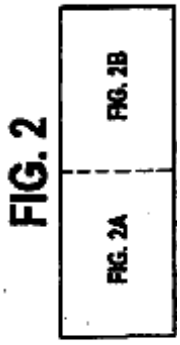


FIG. 2B

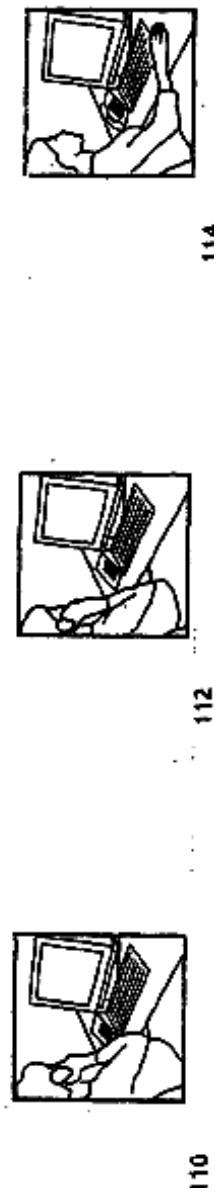
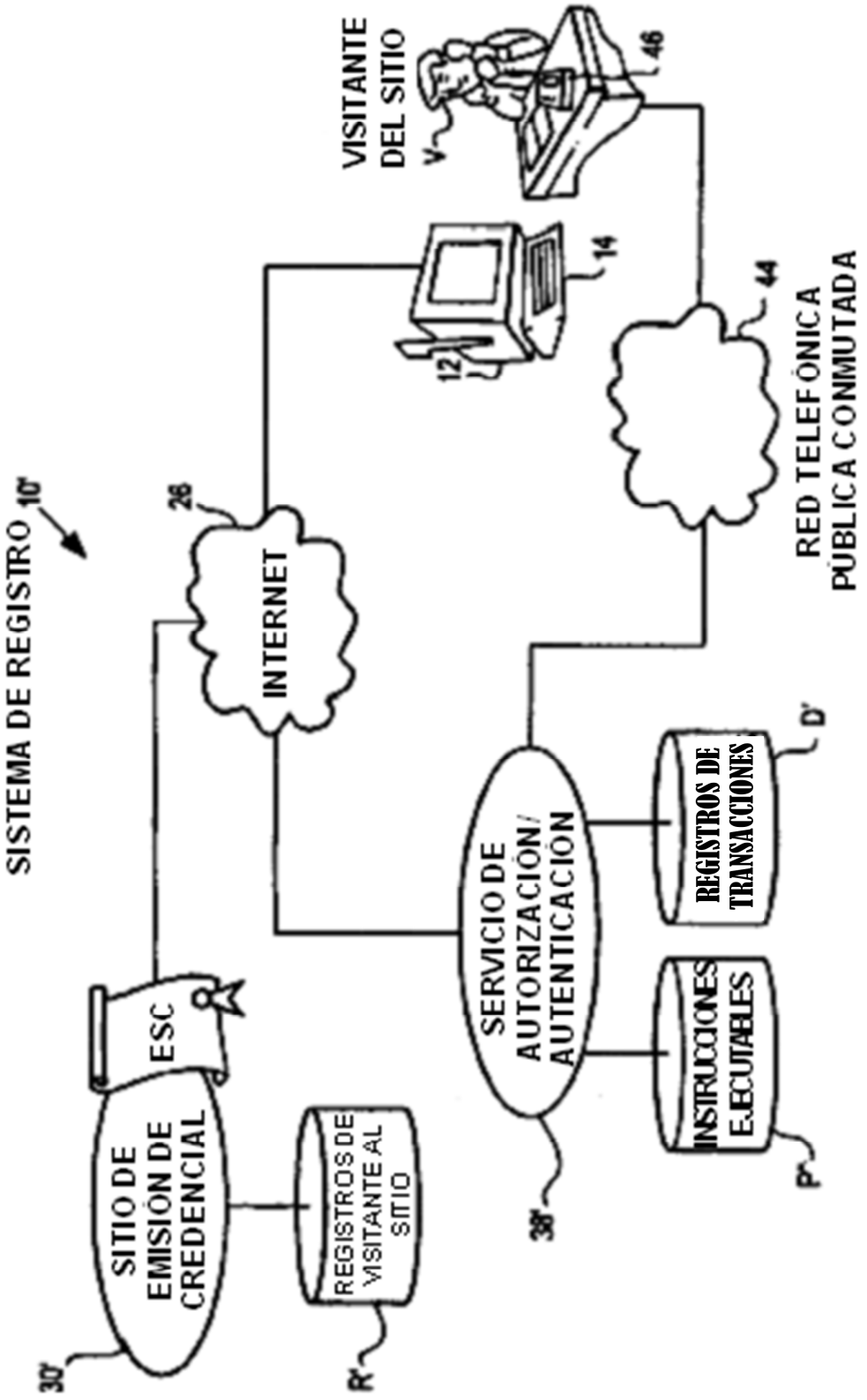


FIG. 3


SISTEMA DE REGISTRO 10'
INTERNET
26
VISITANTE DEL SITIO
V'
46
14
12'
44
RED TELEFÓNICA PÚBLICA CONMUTADA
ESC
SITIO DE EMISIÓN DE CREDENCIAL
30'
REGISTROS DE VISITANTE AL SITIO
R'
SERVICIO DE AUTORIZACIÓN/ AUTENTICACIÓN
38'
REGISTROS DE TRANSACCIONES
D'
INSTRUCCIONES EJECUTABLES
P'

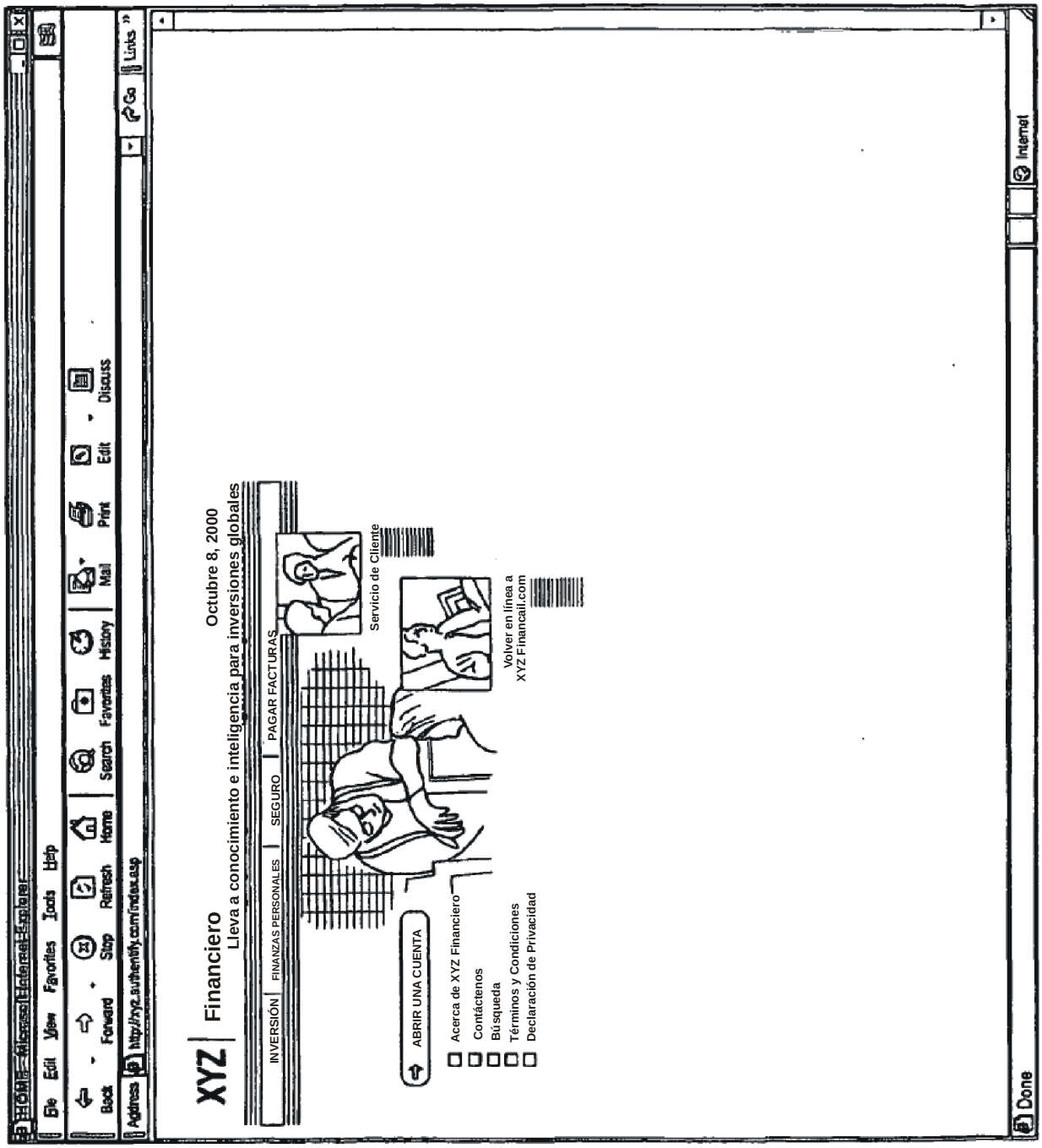

Financiero
Lleva a conocimiento e inteligencia para inversiones globales
Octubre 8, 2000
INVERSIÓN
FINANZAS PERSONALES
SEGURO
PAGAR FACTURAS
Servicio de Cliente
ABRIR UNA CUENTA
Acerca de XYZ Financiero
Contáctenos
Búsqueda
Términos y Condiciones
Declaración de Privacidad
Volver en línea a XYZ Financail.com
Done
Internet

FIG. 4

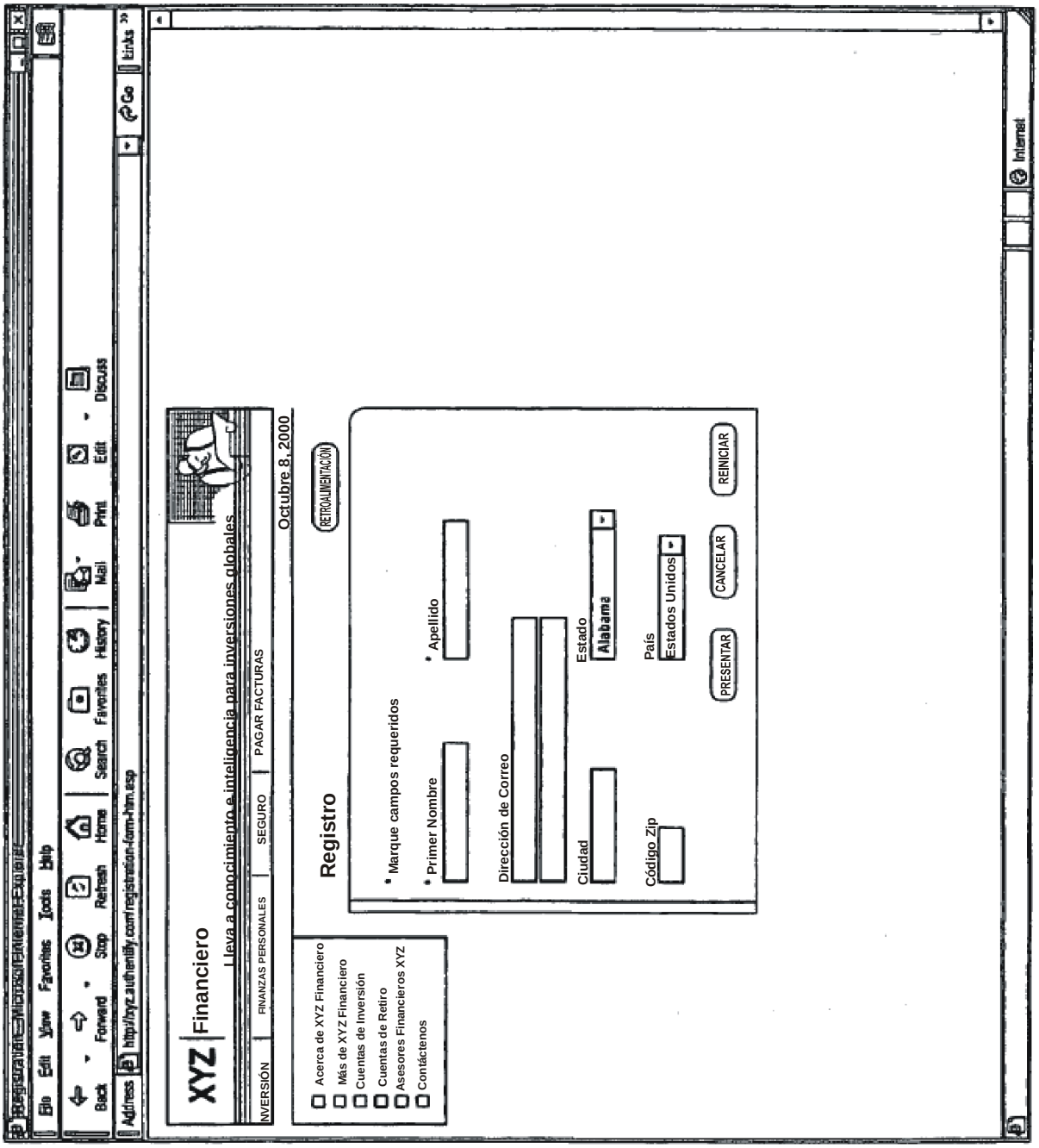
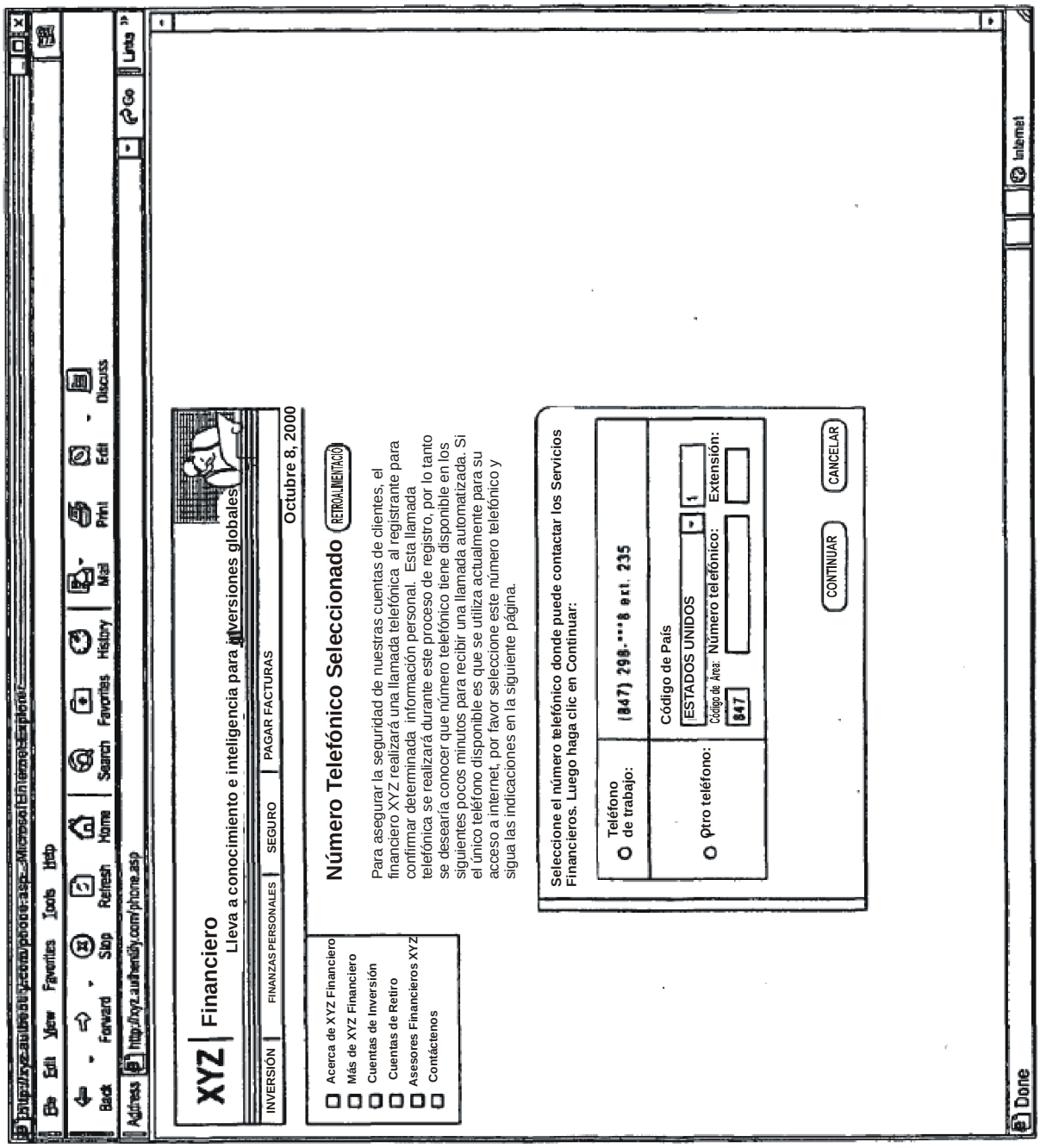

XYZ Financiero
Lleva a conocimiento e inteligencia para inversiones globales
INVERSIÓN
FINANZAS PERSONALES
SEGURO
PAGAR FACTURAS
Octubre 8, 2000
Acerca de XYZ Financiero
Más de XYZ Financiero
Cuentas de Inversión
Cuentas de Retiro
Asesores Financieros XYZ
Contáctenos
Registro
RETROALIMENTACIÓN
* Marque campos requeridos
* Primer Nombre
* Apellido
Dirección de Correo
Ciudad
Estado
Alabama
País
Estados Unidos
Código Zip
PRESENTAR
CANCELAR
REINICIAR

FIG. 5

FIG. 6


XYZ Financiero
Lleva a conocimiento e inteligencia para inversiones globales
INVERSIÓN
FINANZAS PERSONALES
SEGURO
PAGAR FACTURAS
Octubre 8, 2000
Acerca de XYZ Financiero
Más de XYZ Financiero
Cuentas de Inversión
Cuentas de Retiro
Asesores Financieros XYZ
Contáctenos
Número Telefónico Seleccionado
RETROALIMENTACIÓN
Para asegurar la seguridad de nuestras cuentas de clientes, el financiero XYZ realizará una llamada telefónica al registrante para confirmar determinada información personal. Esta llamada telefónica se realizará durante este proceso de registro, por lo tanto se desearía conocer que número telefónico tiene disponible en los siguientes pocos minutos para recibir una llamada automatizada. Si el único teléfono disponible es que se utiliza actualmente para su acceso a internet, por favor seleccione este número telefónico y sigua las indicaciones en la siguiente página.
Seleccione el número telefónico donde puede contactar los Servicios Financieros. Luego haga clic en Continuar:
Teléfono de trabajo:
(847) 298-****
ext. 235
Otro teléfono:
Código de País
ESTADOS UNIDOS
Código de Área:
847
Número telefónico:
Extensión:
CONTINUAR
CANCELAR
Done
Internet

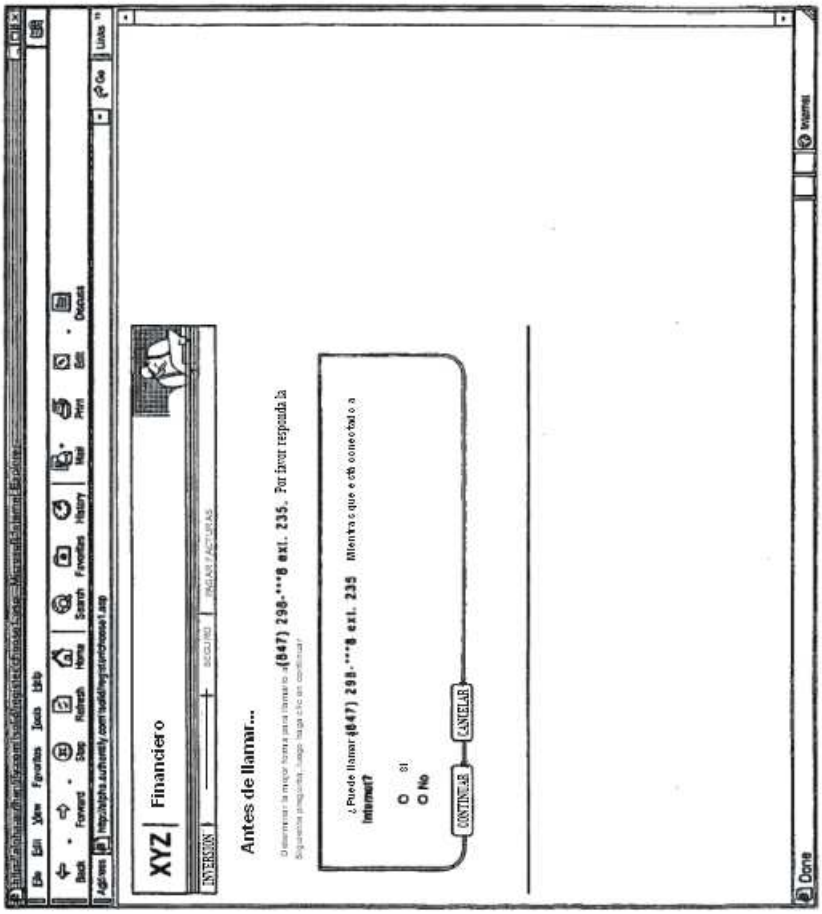
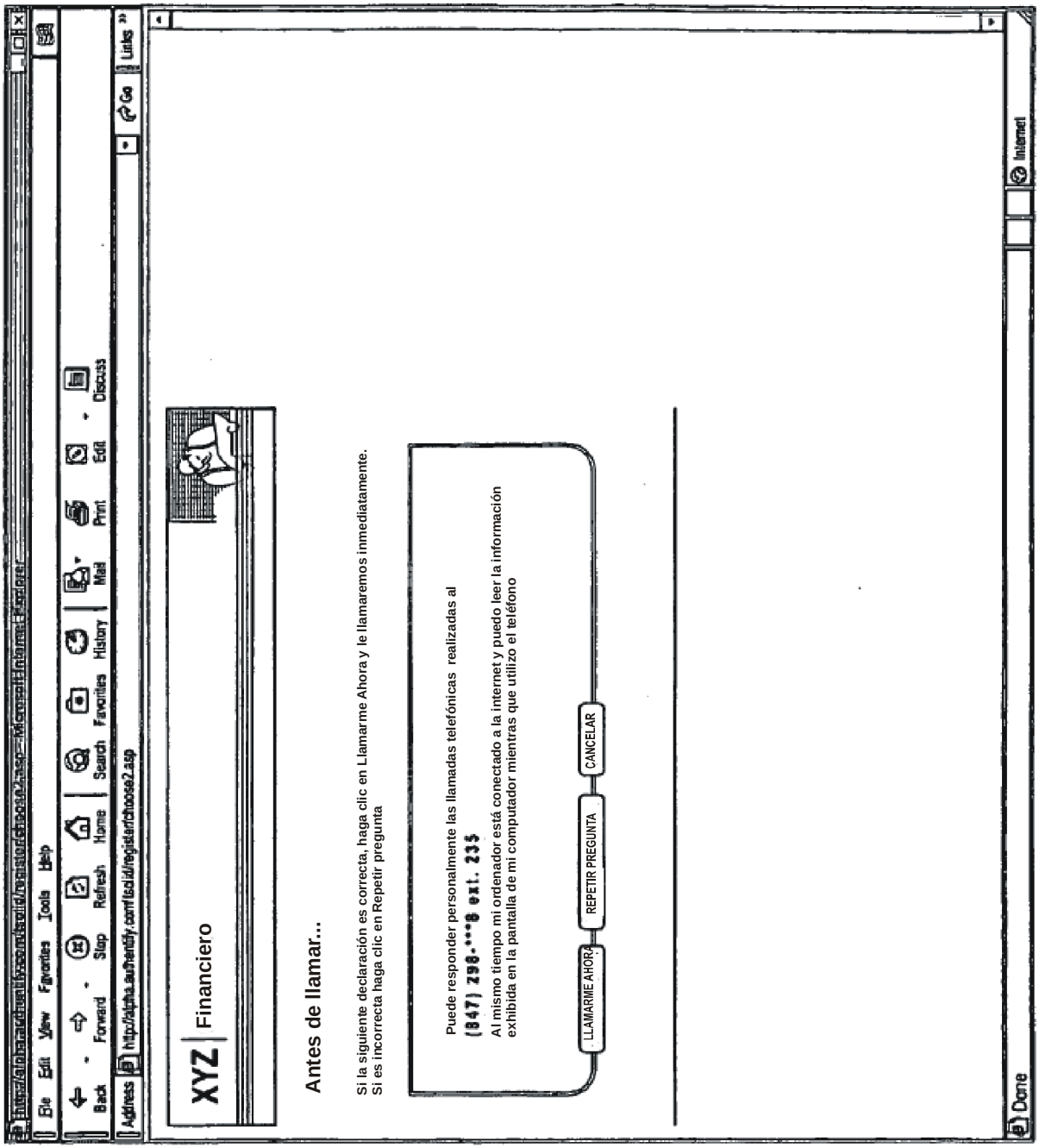

XYZ Financiero
INVERSIÓN
SEGURO
PAGAR FACTURAS
Antes de llamar...
¿Puede llamar (847) 298-***8 ext. 235 Mientras que está conectado a Internet?
Sí
No
CONTINUAR
CANCELAR
Done
Internet

FIG. 7

FIG. 8


XYZ | Financiero
Antes de llamar...
Si la siguiente declaración es correcta, haga clic en Llamarme Ahora y le llamaremos inmediatamente.
Si es incorrecta haga clic en Repetir pregunta
Puede responder personalmente las llamadas telefónicas realizadas al
(847) 298-***8 ext. 235
Al mismo tiempo mi ordenador está conectado a la internet y puedo leer la información exhibida en la pantalla de mi computador mientras que utilizo el teléfono
LLAMARME AHORA
REPETIR PREGUNTA
CANCELAR

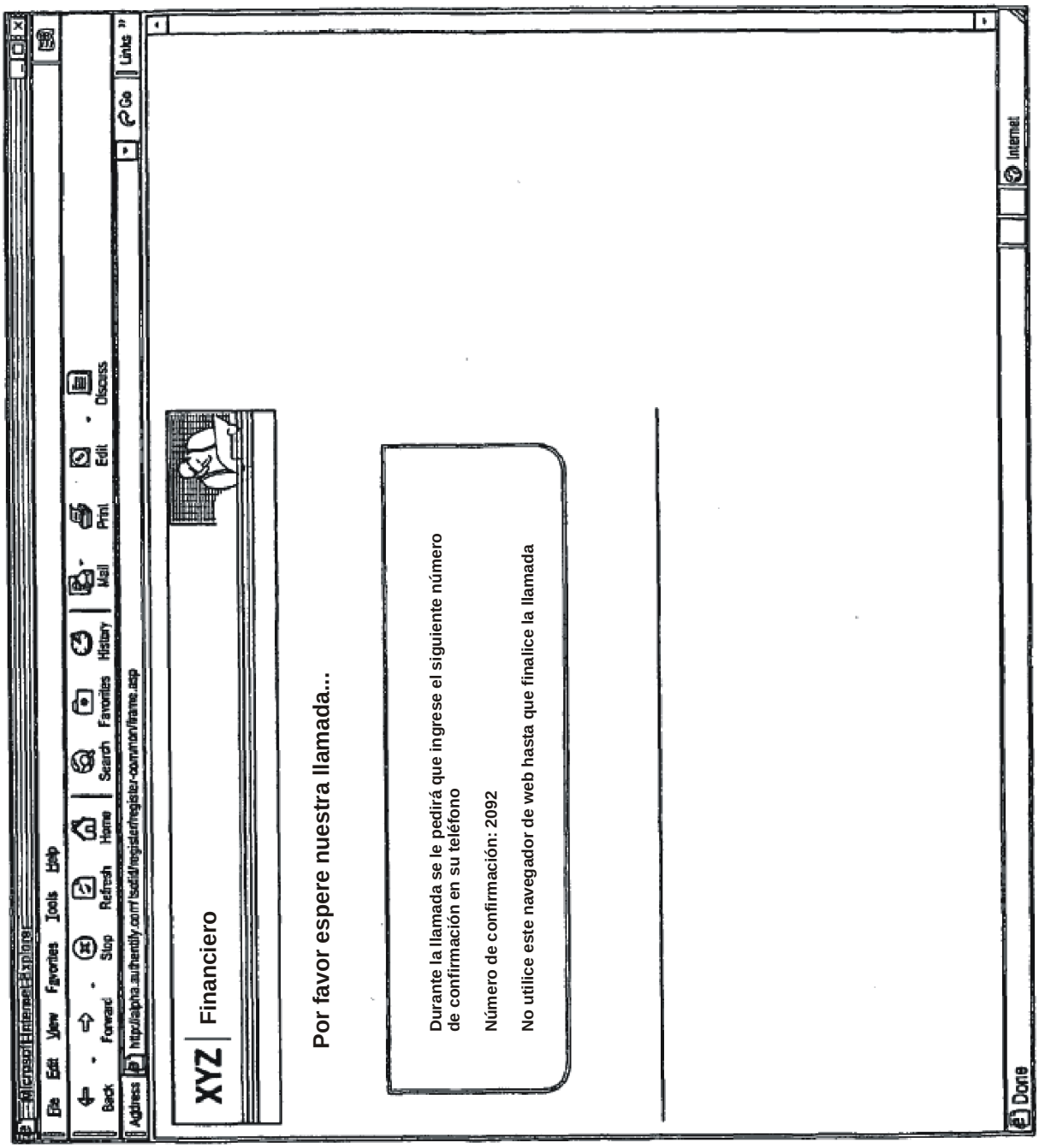

Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://alpha.authentify.com/1sxfd/register/register-consumer/iframe.asp
Go Links
XYZ | Financiero
Por favor espere nuestra llamada...
Durante la llamada se le pedirá que ingrese el siguiente número de confirmación en su teléfono
Número de confirmación: 2092
No utilice este navegador de web hasta que finalice la llamada
Done
Internet

FIG. 9

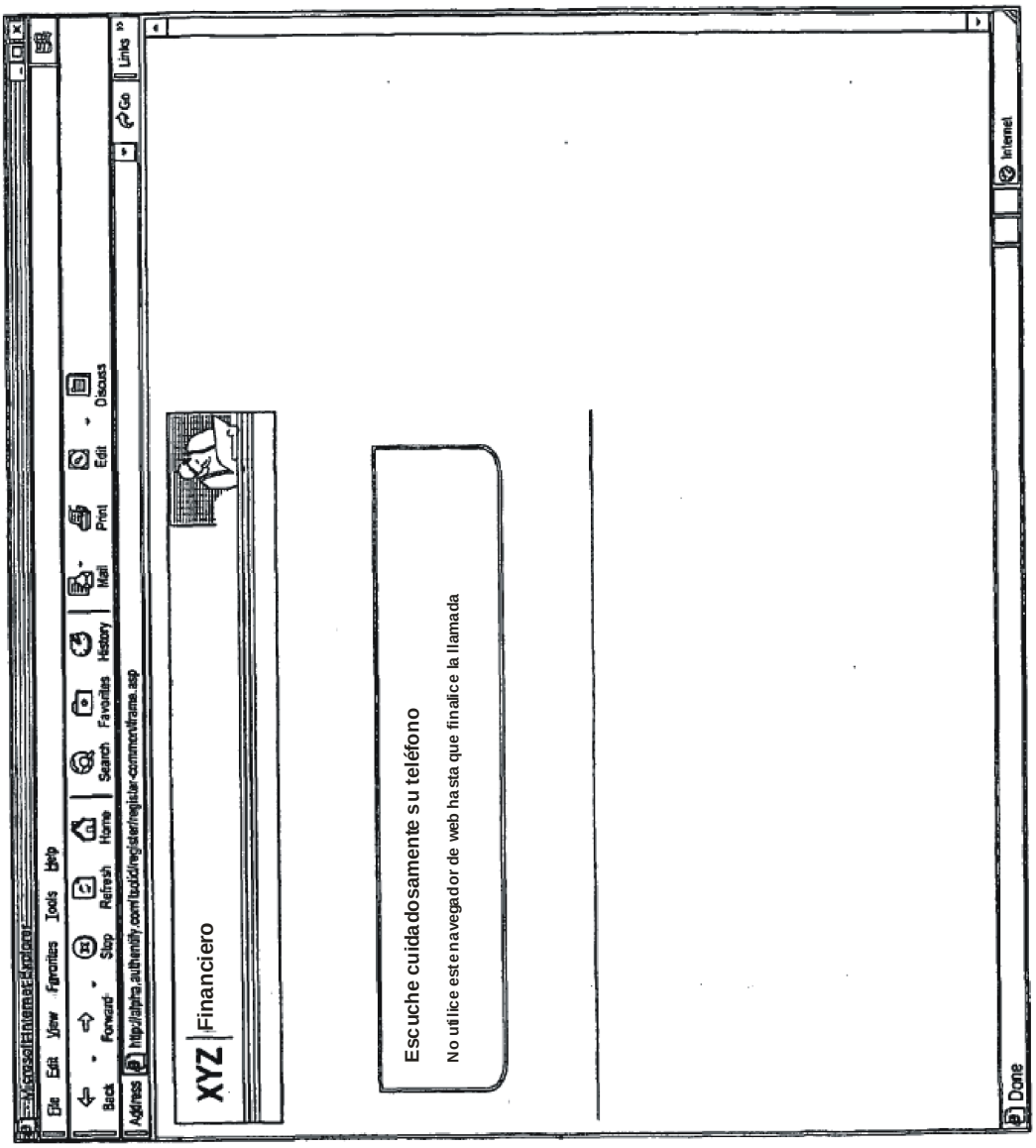

Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Discuss
Links
Address
http://alpha.authentify.com/tauoid/register/registar-commonviframe.asp
XYZ | Financiero
Escuche cuidadosamente su teléfono
No utilice este navegador de web hasta que finalice la llamada
Done
Internet

FIG. 10

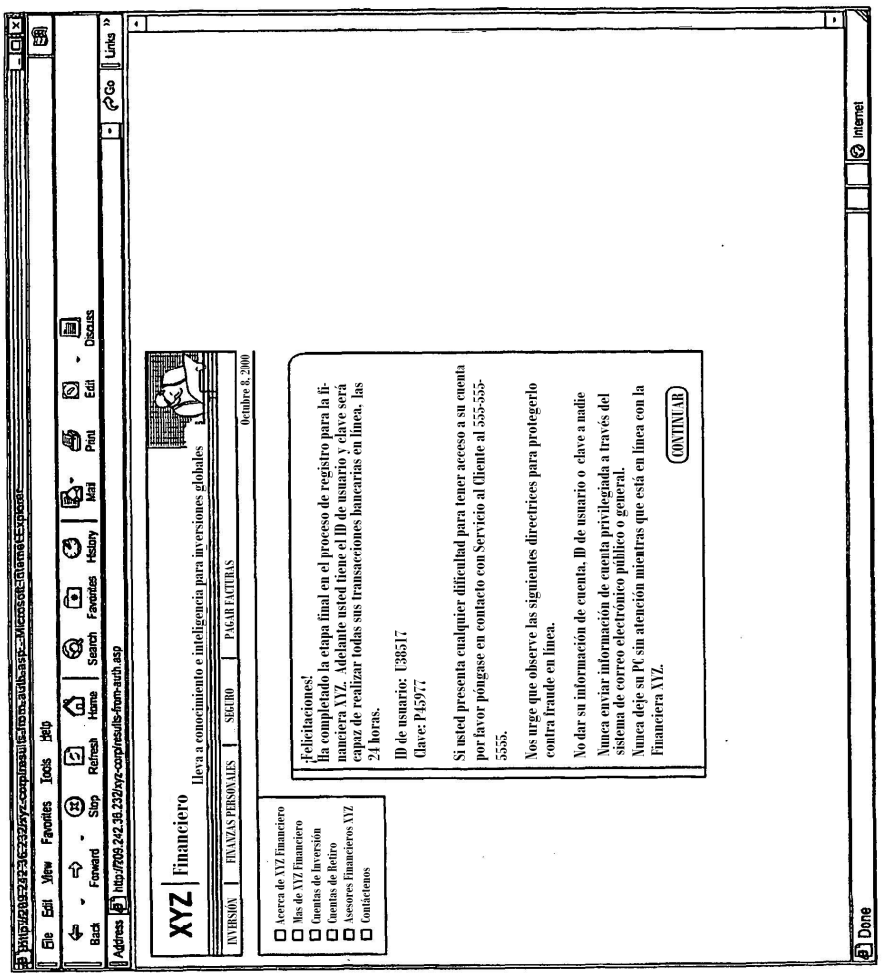

File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://709.242.36.232/xyz-corp/results/trans-auth.asp
Links
XYZ Financiero
Lleva a conocimiento e inteligencia para inversiones globales
INVERSIÓN | FINANZAS PERSONALES | SEGURO | PAGAR FACTURAS
Octubre 8, 2000
Acerca de XYZ Financiero
Mas de XYZ Financiero
Cuentas de Inversión
Cuentas de Retiro
Asesores Financieros XYZ
Contáctenos
¡Felicitaciones!
Ha completado la etapa final en el proceso de registro para la financiera XYZ. Adelante usted tiene el ID de usuario y clave será capaz de realizar todas sus transacciones bancarias en línea, las 24 horas.
ID de usuario: U38517
Clave: P45977
Si usted presenta cualquier dificultad para tener acceso a su cuenta por favor póngase en contacto con Servicio al Cliente al 555-555-5555.
Nos urge que observe las siguientes directrices para protegerlo contra fraude en línea.
No dar su información de cuenta, ID de usuario o clave a nadie
Nunca enviar información de cuenta privilegiada a través del sistema de correo electrónico público o general.
Nunca deje su PC sin atención mientras que está en línea con la Financiera XYZ.
CONTINUAR
Done
Internet

FIG. 11

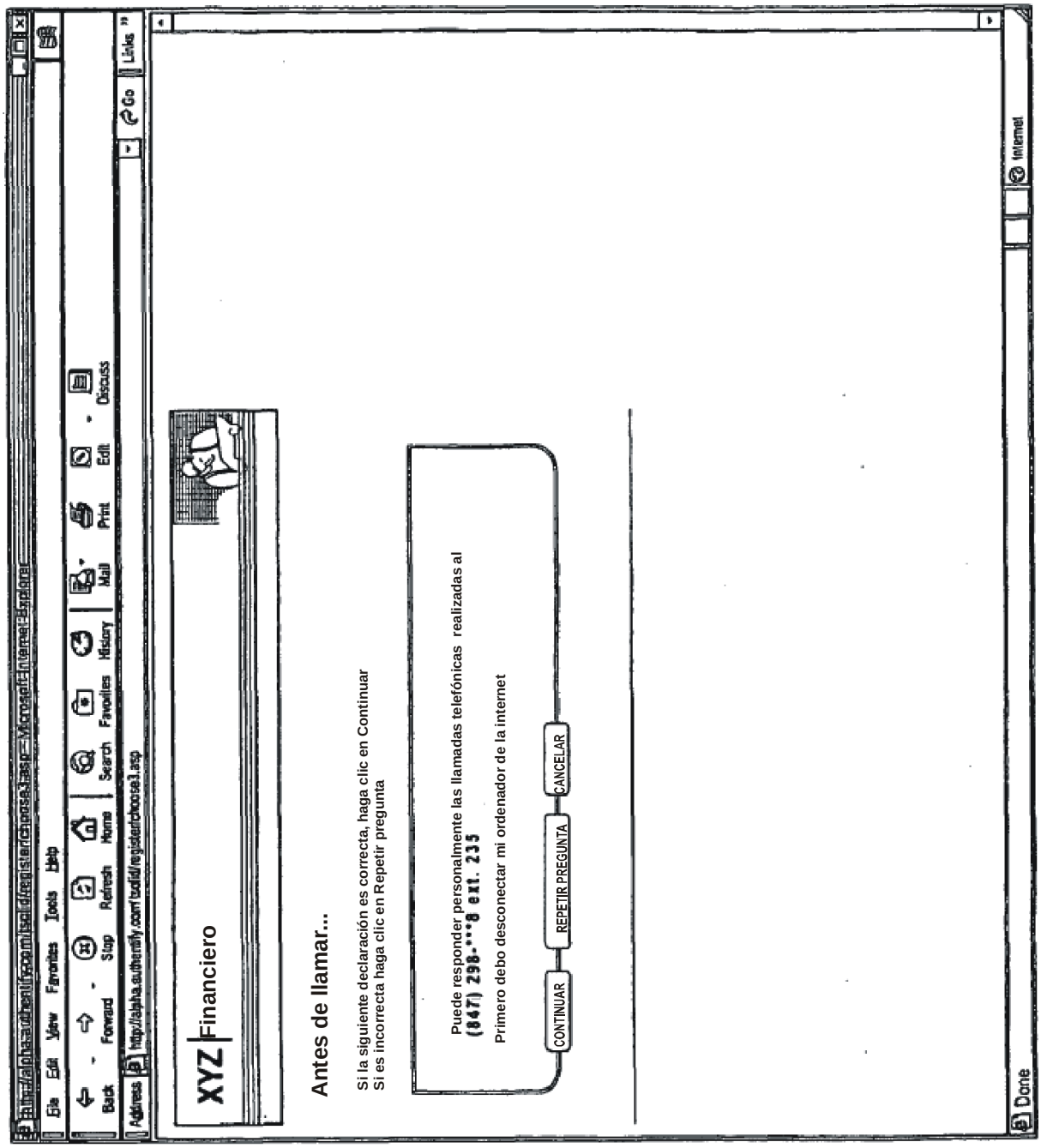

XYZ Financiero
Antes de llamar...
Si la siguiente declaración es correcta, haga clic en Continuar
Si es incorrecta haga clic en Repetir pregunta
Puede responder personalmente las llamadas telefónicas realizadas al
(847) 298-***8 ext. 235
Primero debo desconectar mi ordenador de la internet
CONTINUAR
REPETIR PREGUNTA
CANCELAR

FIG. 12

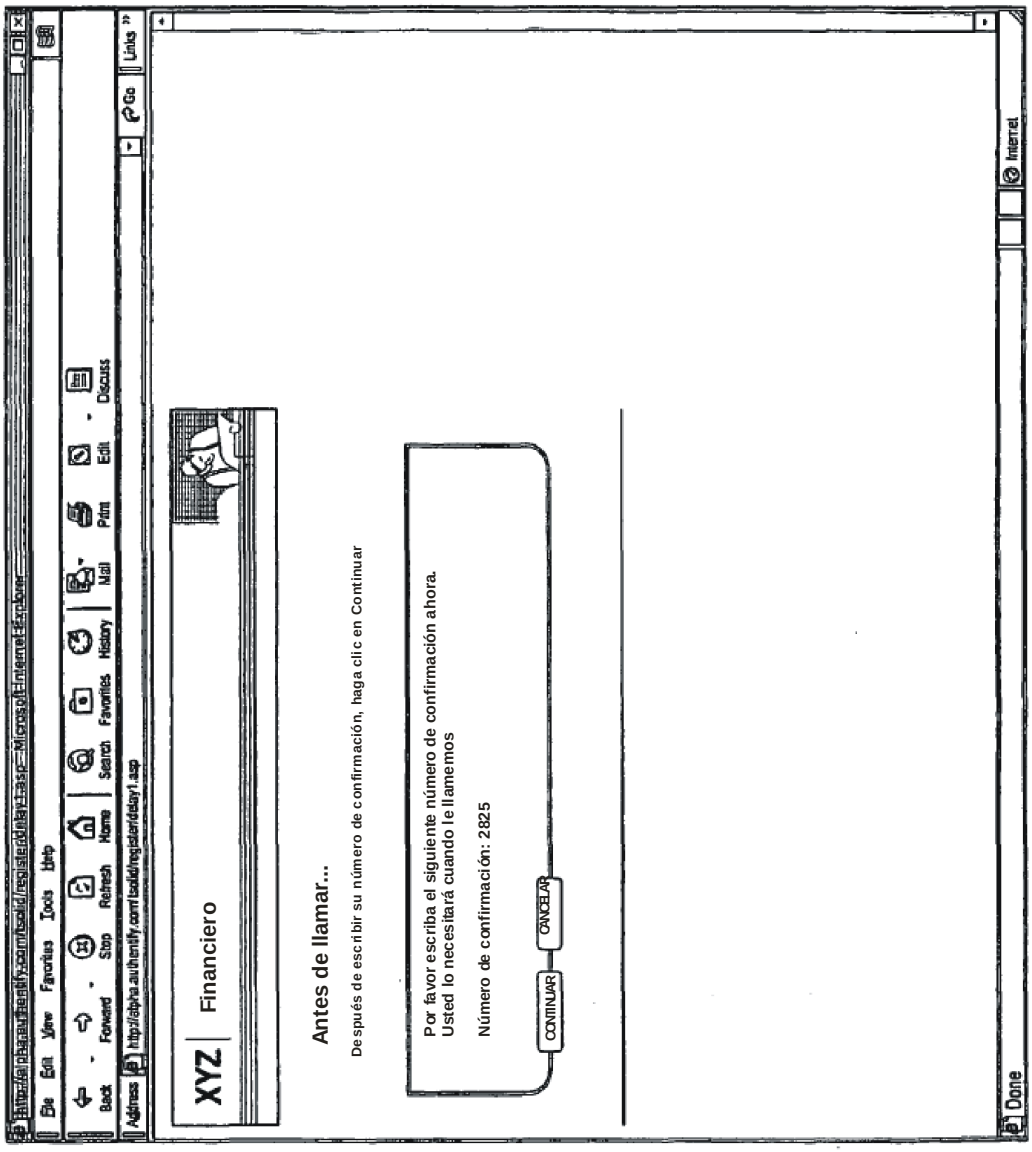

XYZ
Financiero
Antes de llamar...
Después de escribir su número de confirmación, haga clic en Continuar
Por favor escriba el siguiente número de confirmación ahora.
Usted lo necesitará cuando le llamemos
Número de confirmación: 2825
CONTINUAR
CANCELAR
Done
Internet

FIG. 13

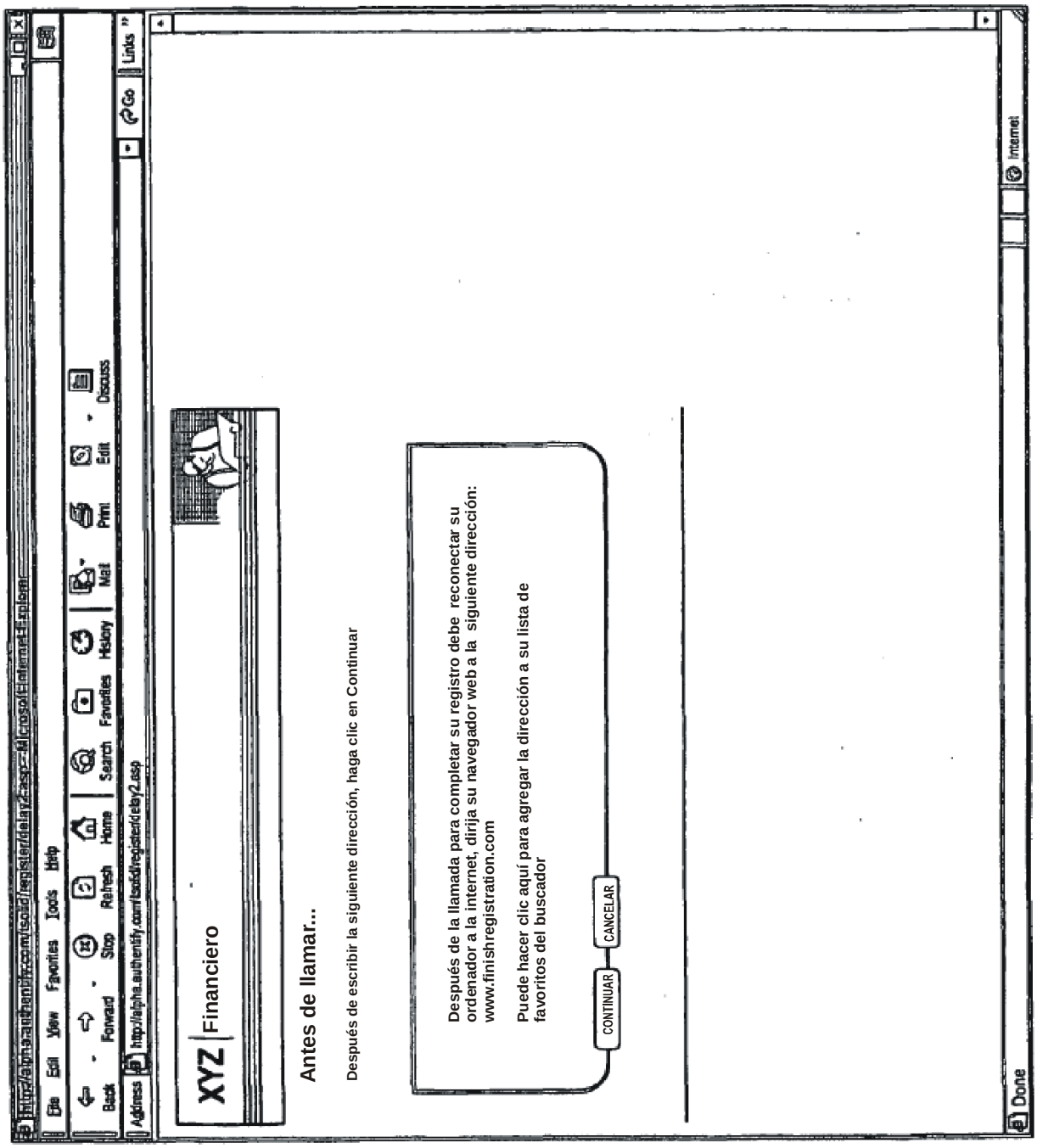

File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://alpha.authentify.com/bank/register/delay2.asp
Links
Go
XYZ Financiero
Antes de llamar...
Después de escribir la siguiente dirección, haga clic en Continuar
Después de la llamada para completar su registro debe reconectar su ordenador a la internet, dirija su navegador web a la siguiente dirección: www.finishregistration.com
Puede hacer clic aquí para agregar la dirección a su lista de favoritos del buscador
CONTINUAR
CANCELAR
Done
Internet

FIG. 14

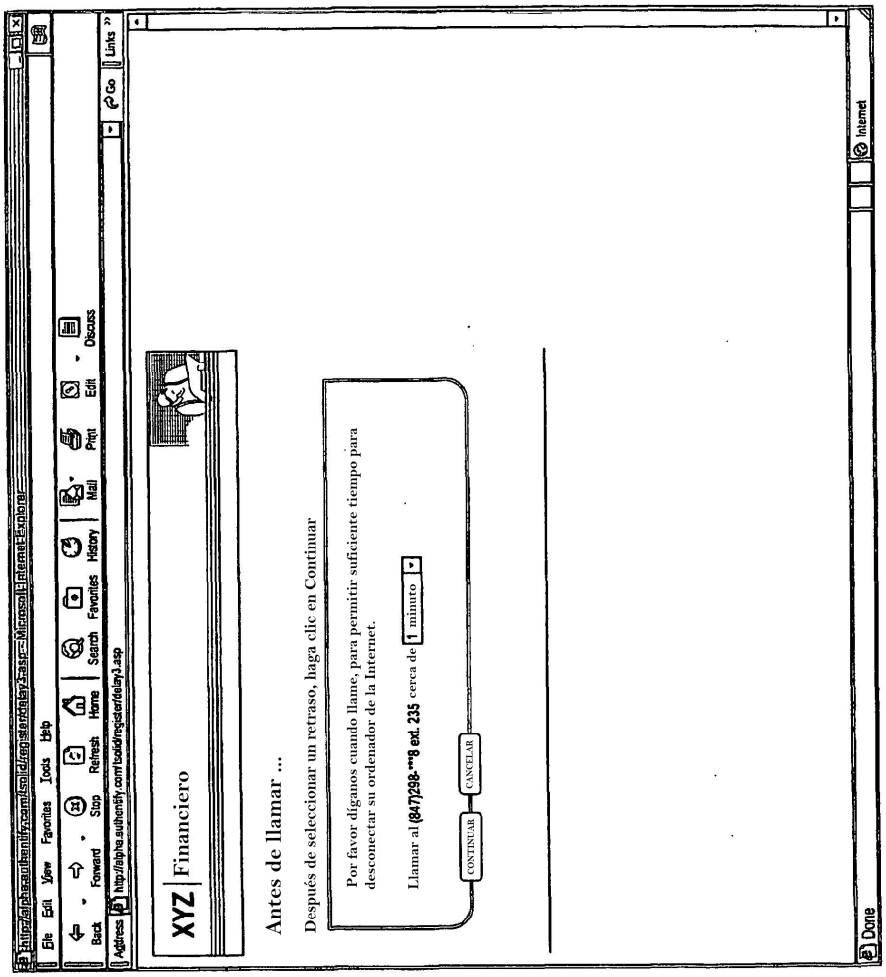

XYZ Financiero
Antes de llamar ...
Después de seleccionar un retraso, haga clic en Continuar
Por favor díganos cuando llame, para permitir suficiente tiempo para desconectar su ordenador de la Internet.
Llamar al (847)298-***8 ext. 235 cerca de 1 minuto
CONTINUAR
CANCELAR

FIG. 15

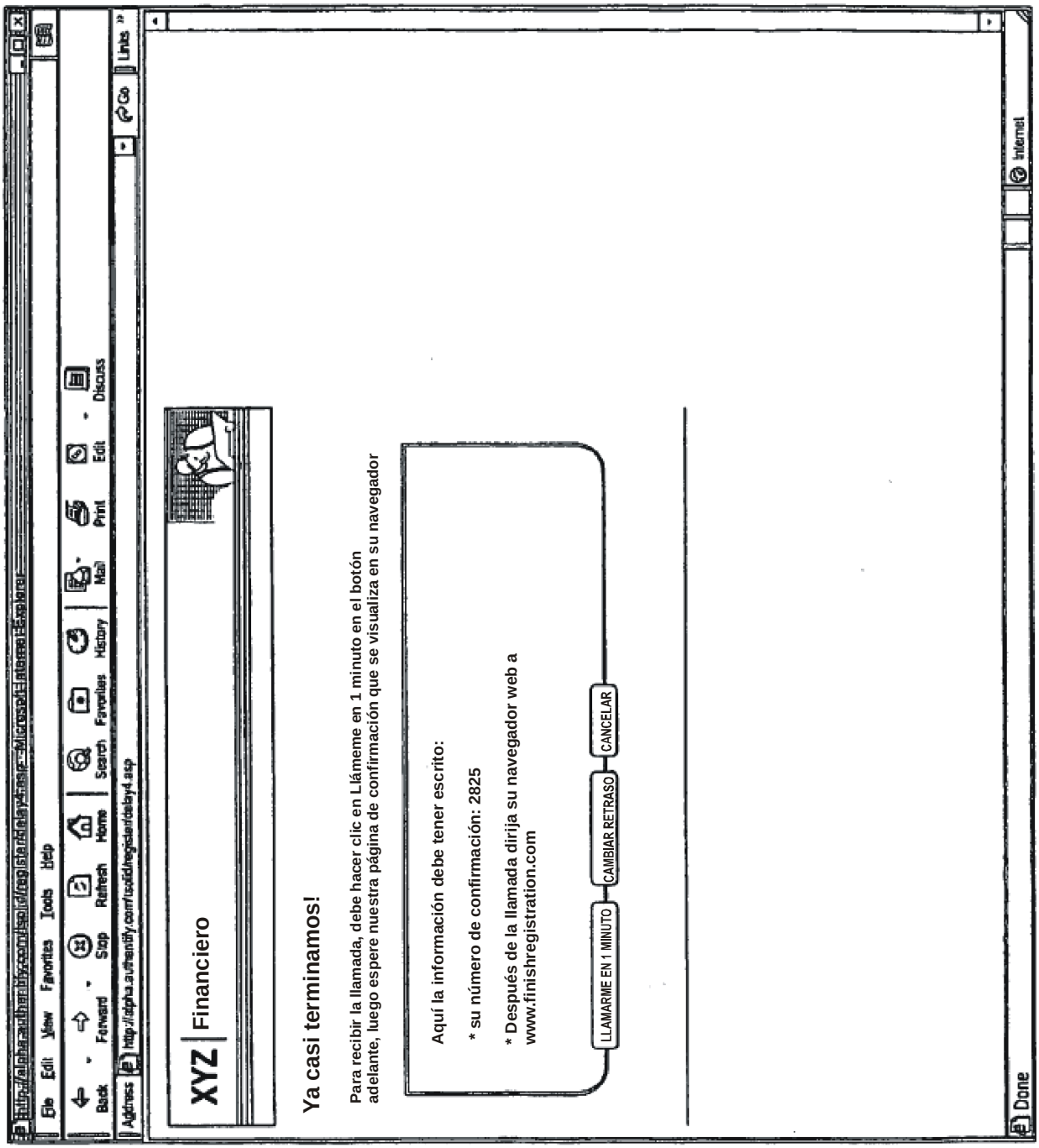

XYZ Financiero
Ya casi terminamos!
Para recibir la llamada, debe hacer clic en Llámeme en 1 minuto en el botón adelante, luego espere nuestra página de confirmación que se visualiza en su navegador
Aquí la información debe tener escrito:
* su número de confirmación: 2825
* Después de la llamada dirija su navegador web a www.finishregistration.com
LLAMARME EN 1 MINUTO
CAMBIAR RETRASO
CANCELAR

FIG. 16

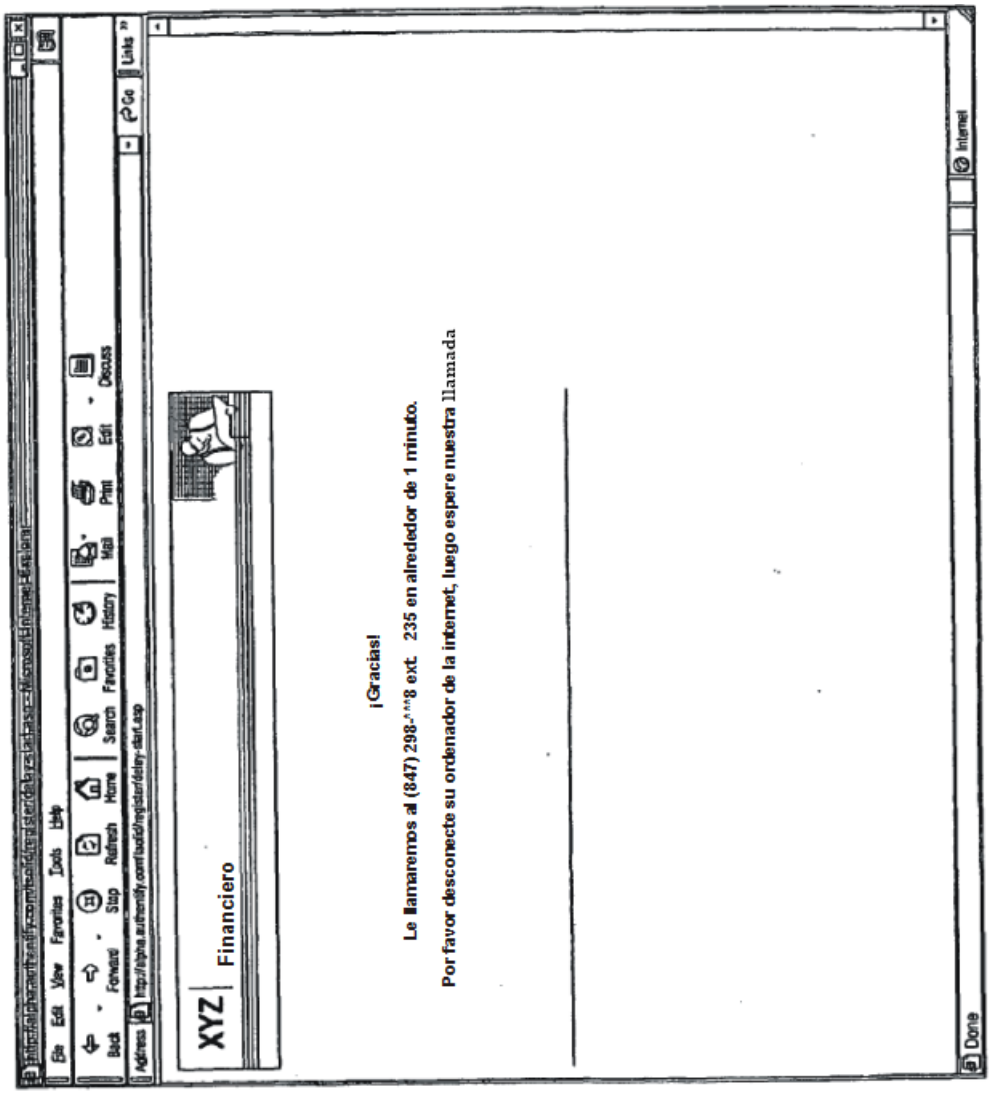

XYZ | Financiero
¡Gracias!
Le llamaremos al (847) 298-****8 ext. 235 en alrededor de 1 minuto.
Por favor desconecte su ordenador de la internet, luego espere nuestra llamada

FIG. 17