

MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

5

[0001] La presente solicitud reivindica la prioridad y el beneficio de la solicitud de patente provisional de propiedad común, U.S. Serie N°. 62/045,449, titulada "MONITOREO ANTI-FRAUDE, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN DEL CENTRO DE LLAMADAS", con fecha de presentación el 3 de septiembre, 10 2014, y que tiene número de expediente de abogado TELP-0002-00.00US, que se incorpora aquí como referencia en su totalidad.

ANTECEDENTES

15 [0002] Un centro de llamadas gestiona grandes volúmenes de solicitudes por teléfono u otro medio análogo de tecnologías de la comunicación. Por ejemplo, estos centros de llamadas se establecen para proporcionar apoyo y/o información a los llamantes con respecto a productos y/o servicios. El centro de llamadas se puede operado por la compañía asociada con el producto o servicio, o un tercero 20 asignado para proporcionar soporte al cliente. Como ventaja, el manejo colectivo de las llamadas a través de una red de estaciones de trabajo con servicio de representantes o agentes promueve un enfoque práctico cuando se trata con clientes en que el centro de llamadas está configurado para permitir un gran número de llamadas a ser manejadas a título personal.

25

[0003] En una implementación, un centro de llamadas entrantes gestiona las llamadas entrantes para proporcionar servicios a las llamadas entrantes. Por ejemplo, un centro entrante puede proporcionar soporte para completar una venta,

manejar asuntos y problemas con productos (e.g., instrucciones de instalación,
30 servicio de garantía, etc.), manejar llamadas relacionadas con servicios (e.g.,
banca, colecciones, policía, incendio, alarma, etc.) y otros tipos de servicios
similares.

[0004] En otra implementación, un centro de llamadas saliente inicia llamadas.
35 Por ejemplo, el centro se puede configurado para proporcionar telemarketing para
un producto o servicio, permitir la solicitud de donaciones caritativas o políticas,
proporcionar servicios de cobro de deudas, realizar encuestas o estudios de
mercado, etc.

40 **[0005]** Muchos centros de llamadas individualizados están centralizados para
proporcionar espacio para muchos agentes. Por ejemplo, un centro de llamadas
más grande puede soportar cientos o miles de estaciones de trabajo en un solo
edificio o campus de edificios. De esta manera, el mantenimiento e instalación de
toda la infraestructura (e.g., computadores, cubículo de estación de trabajo, etc.)
45 está centralizado.

[0006] El centro de llamadas puede representar un cliente de terceros, en el
que el agente gestiona las llamadas de los clientes en nombre del cliente de
terceros. Como tal, el agente puede estar autorizado a acceder a información
50 privilegiada del cliente utilizando las bases de datos del cliente. Por ejemplo, el
cliente se puede una institución bancaria y el agente está manejando una llamada
para ayudar a un cliente a determinar el saldo de su cuenta. En ese caso, el
agente puede acceder a los datos personales del cliente controlados por la
institución bancaria para proporcionar un saldo de cuenta.

55

[0007] Sin embargo, hay casos en los que el agente accede a información privilegiada del cliente cuando no hay necesidad legítima. Es decir, mientras que un agente del centro de llamadas inherentemente ha autorizado el acceso a la información personal e identificable, el agente debe utilizar solamente este acceso con base en la necesidad de tener acceso. Cuando se está produciendo una actividad fraudulenta, no sólo el agente puede recopilar información personal crítica a través del acceso no autorizado, sino que esa información se puede utilizada posteriormente para cometer fraude adicional (e.g., solicitar crédito, realizar transacciones de compra, etc.).

[0008] Lo que se necesita es una forma de combatir el fraude en un centro de atención telefónica.

RESUMEN

[0009] En implementaciones de la presente invención, se describe un método implementado por computador para detectar fraudes. En otras implementaciones, se describe un medio no transitorio legible por computador que tiene instrucciones ejecutables por computador para hacer que un sistema de cómputo realice un método para detectar fraude. En otras implementaciones, se describe un sistema de cómputo que comprende un computador y una memoria acoplados al procesador y que tiene almacenadas en él instrucciones que, si son ejecutadas por el sistema de cómputo, hacen que el sistema de cómputo ejecute un método para detectar fraude. El método incluye determinar que un primer agente en una primera estación de trabajo de un centro de contacto no está implicado en una interacción con un cliente (e.g., en una llamada hecha por primera vez). El centro de contacto incluye una pluralidad de estaciones de trabajo atendidos por una pluralidad de agentes. El método incluye determinar que el primer agente está

accediendo a un recurso con base en el cliente por primera vez. El recurso está
85 asociado con un cliente y, por ejemplo, puede incluir información personal e
identificable que está asociada con uno o más clientes y/o individuos, en donde la
información se puede utilizada por el agente para realizar una actividad
fraudulenta. Cuando se detecta la actividad fraudulenta potencial, el método
incluye recolección de evidencia electrónica de la primera estación de trabajo,
90 donde la evidencia se puede usada para probar el fraude real por el agente.

[00010] En otra implementación, se implementa un método por computador
para detectar actividad fraudulenta potencial en una estación de trabajo y para
tomar medidas preventivas una vez que se detecta una actividad fraudulenta
95 potencial. En otras implementaciones, se describe un medio no transitorio legible
por computador que tiene instrucciones ejecutables por computador para hacer
que un sistema de cómputo realice un método para detectar actividad fraudulenta
potencial en una estación de trabajo y para tomar medidas preventivas una vez
que se detecta actividad fraudulenta potencial. En otras implementaciones, se
100 describe un sistema de cómputo que comprende un computador y una memoria
acoplados al procesador y que tiene almacenadas en él instrucciones que, si son
ejecutadas por el sistema de cómputo, hacen que el sistema de cómputo ejecute
un método para detectar actividad fraudulenta potencial en una estación de trabajo
y para tomar medidas preventivas una vez que se detecta una actividad
105 fraudulenta potencial. El método incluye determinar que una actividad fraudulenta
potencial se lleva a cabo en un centro de contacto que comprende una pluralidad
de estaciones de trabajo atendidas por una pluralidad de agentes. El método
incluye determinar la actividad fraudulenta potencial que se produce en una
primera estación de trabajo. El método incluye proporcionar una notificación del
110 evento de la actividad fraudulenta potencial en un gráfico del centro de contacto,
en el que el gráfico del centro de contacto indica las ubicaciones de cada estación

de trabajo y la información del estado para cada estación de trabajo. El método incluye capturar al menos una imagen de la primera estación de trabajo.

115 **[00011]** En otra implementación más, se describe un sistema de estaciones de trabajo de monitoreo de un centro de contacto. El sistema incluye una pluralidad de estaciones de trabajo de una sección de un centro de contacto, donde cada estación de trabajo comprende un sistema de cómputo configurado para acceder a recursos de un cliente a través de una primera red de comunicación. La pluralidad de estaciones de trabajo es atendida por una pluralidad de agentes. El sistema incluye una pluralidad de monitores asociados con la pluralidad de estaciones de trabajo, donde un primer sistema de cálculo de una primera estación de trabajo comprende un primer monitor configurado para rastrear la actividad realizada por un agente en el primer sistema de cómputo. El sistema incluye un centro de seguridad acoplado a la pluralidad de monitores a través de una segunda red de comunicaciones. El centro de seguridad está configurado para recibir de la pluralidad de monitores información relacionada con una pluralidad de actividades de una pluralidad de sistema de cómputo asociado con la pluralidad de estaciones de trabajo. El sistema incluye un gráfico que identifica la pluralidad de estaciones de trabajo, en el que el centro de seguridad genera y gestiona el gráfico con base en la información recibida. El sistema incluye un primer icono que representa una primera estación de trabajo en el gráfico, en el que el icono está configurado para proporcionar un estado (e.g., estado de inicio de sesión, etc.) de un agente que atiende a la primera estación de trabajo.

135

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[00012] Los dibujos adjuntos, que se incorporan y forman parte de esta especificación y en los que los mismos números representan elementos similares,

140 ilustran implementaciones de la presente descripción y, junto con la descripción,
sirven para explicar los principios de la descripción.

[00013] La FIG. 1 ilustra un diagrama de bloques de un sistema de cómputo de
ejemplo adecuado para hacer implementaciones de acuerdo con la presente
145 descripción.

[00014] La FIG. 2 es una ilustración de un sistema configurado para identificar
la actividad fraudulenta potencial realizada por un agente dentro de un centro de
contacto y tomar acción preventiva una vez que se ha identificado la actividad, de
150 acuerdo con una implementación de la presente descripción.

[00015] La FIG. 3 es un diagrama de bloques de los componentes de una
estación de trabajo del centro de contacto que está configurada para monitorear la
actividad de un agente del centro de contacto con el fin de identificar la actividad
155 fraudulenta potencial realizada por el agente, de acuerdo con una implementación
de la presente descripción.

[00016] La FIG. 4 es un diagrama de flujo que ilustra un método para detectar
actividad fraudulenta y tomar medidas preventivas una vez que se detecta la
160 actividad fraudulenta potencial, de acuerdo con una implementación de la presente
descripción.

[00017] La FIG. 5A es un diagrama que ilustra un piso del centro de contacto
que incluye una pluralidad de estaciones de trabajo, y un sistema de monitor de
165 vídeo configurado para ver cada una de las estaciones de trabajo, de acuerdo con
una implementación de la presente descripción.

[00018] La FIG. 5B es un diagrama que ilustra una disposición típica de recursos disponibles para una estación de trabajo del centro de contacto y un dispositivo de captura de vídeo configurado y orientado para capturar una vista frontal de un agente que atiende a la estación de trabajo cuando instruye, tal que las imágenes de la estación de trabajo se capturan cuando la actividad fraudulenta potencial se detecta en esa estación de trabajo, de acuerdo con una implementación de la presente descripción.

[00019] La FIG. 6 es un diagrama de flujo que ilustra un método para realizar detección de fraude, de acuerdo con una implementación de la presente descripción.

[00020] La FIG. 7A es un diagrama de un gráfico que ilustra estaciones de trabajo y sus ubicaciones dentro de una sección o piso del centro de contacto, en el que los iconos que representan las estaciones de trabajo pueden ser aumentados para proporcionar información relacionada con el estado de agentes y/o estaciones de trabajo, así como también información que proporciona notificación cuando se detecta actividad fraudulenta potencial en una o más estaciones de trabajo, de acuerdo con una implementación de la presente descripción.

[00021] Las FIGS. 7B-J son diagramas de varios símbolos que proporcionan información relacionada con el estado de agentes y/o estaciones de trabajo, así como información que proporciona notificación cuando se detecta actividad fraudulenta potencial en una o más estaciones de trabajo, de acuerdo con una implementación de la presente descripción.

DESCRIPCIÓN DETALLADA

[00022] A continuación se hará referencia en detalle a las diversas implementaciones de la presente descripción, cuyos ejemplos se ilustran en los dibujos adjuntos. Aunque se describe en conjunción con estas implementaciones, se entenderá que no se pretende limitar la descripción a estas implementaciones. Por el contrario, la divulgación pretende cubrir alternativas, modificaciones y equivalentes, que se pueden incluir dentro del espíritu y alcance de la descripción como se define en las reivindicaciones adjuntas. Además, en la siguiente descripción detallada de la presente descripción, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de la presente descripción. Sin embargo, se entenderá que la presente descripción se puede practicar sin estos detalles específicos. En otros casos, no se han descrito con detalle métodos bien conocidos, procedimientos, componentes y circuitos para no obscurecer innecesariamente aspectos de la presente descripción.

[00023] Las implementaciones de la presente invención se describen dentro del contexto de un centro de contacto. El centro de contacto está configurado para proporcionar servicios a los clientes en nombre de terceros clientes a través de varios sistemas y métodos de interacción y/o comunicación con el cliente. Las diferentes configuraciones de un centro de contacto incluyen ubicar el centro de contacto de forma remota desde el cliente y/o el cliente, localizar el centro de contacto localmente para el cliente y/o el cliente, etc. En una ilustración de un centro de contacto, en lugar de utilizar empleados del banco, un cliente bancario puede utilizar un centro de contacto para prestar servicios bancarios a sus clientes, en el que los agentes del centro de contacto interactúan directamente con los clientes. Por ejemplo, un centro de llamadas ilustra un tipo del centro de contacto y está configurado para facilitar las interacciones y/o comunicaciones

entre agentes y clientes a través de una red telefónica, como el manejo de
225 llamadas entrantes y salientes.

[00024] Además, un centro de contacto es capaz de manejar cualquier tipo de interacción y/o comunicación entre un agente y un cliente. Un tipo de interacción implica comunicaciones telefónicas entre un agente y un cliente a través de una
230 red telefónica (e.g., red móvil conmutada pública, combinaciones de red conmutada móvil y pública, etc.). Para fines ilustrativos solamente, otros tipos de interacciones y/o comunicaciones entre un agente y un cliente incluyen video, texto, mensajes de texto, comunicaciones basadas en Internet, etc.

[00025] Por consiguiente, las implementaciones de la presente invención proporcionan la capacidad de identificar, recopilar evidencia y evitar el fraude de agentes de contacto con casos de uso específicos en operaciones de centros de contacto. Otras implementaciones de la presente invención alertan o bloquean (dependiendo de ajustes de configuración) acceso fraudulento del agente del
240 centro de contacto para la información personal e identificable del cliente.

[00026] Algunos estrategias dentro de la industria del centro de contacto aceptan el fraude como un costo operativo. Por ejemplo, estos estrategias aceptan que los agentes del centro de contacto pueden abusar de su privilegio de acceder
245 sin autorización a información personal (e.g., salud y finanzas) de los recursos del cliente (e.g., bases de datos) relacionados con los clientes en violación de varias leyes, incluyendo la Ley de Responsabilidad de Portabilidad del Seguro de Salud (HIPPA); aceptan que los agentes actualmente roban información financiera de un cliente para hacer compras para el beneficio del agente del centro de contacto;
250 aceptan que los agentes enviarán a sabiendas artículos de reemplazo bajo garantía a la dirección del agente en lugar de la dirección de un cliente; etc. Estas

estrategas promueven un modelo de negocio insostenible que permite realizar fraude a través de un centro de contacto.

255 **[00027]** El fraude no necesita ser tolerado dentro de la industria del centro de
contacto. El fraude se puede abordado a través de un enfoque de tres puntos,
incluyendo monitoreo, detección y prevención. Específicamente, el primer punto
proporciona el monitoreo de la actividad de los agentes del centro de contacto y/o
la actividad realizada sobre los recursos utilizados por los agentes. La información
260 se puede recogida y analizada en tiempo real o después de la ocurrencia. Por
ejemplo, se puede recopilar un historial de información para un solo agente o un
grupo de agentes, de tal manera que se pueda realizar un análisis estadístico, tal
como determinar promedios estadísticos para diversas actividades. Otras técnicas
de recolección también están bien apoyadas. El segundo dato prevé la detección
265 de una posible actividad fraudulenta basada en la información recopilada. Por
ejemplo, cierta actividad puede coincidir con un patrón de actividad que se sabe
que está asociado con actividad fraudulenta. En otros ejemplos más, las
actividades de un agente pueden estar fuera de las normas estadísticas asociadas
con un grupo de agentes y pueden indicar una actividad fraudulenta potencial. Una
270 vez que se ha señalado la actividad fraudulenta potencial de un agente, se puede
llevar a cabo una investigación adicional para determinar si se ha llevado a cabo
una actividad fraudulenta real. El tercer punto proporciona la prevención de la
actividad fraudulenta. La prevención incluye el conocimiento por el cuerpo de
agentes que están siendo monitoreados, lo que proporciona un elemento de
275 disuasión. La prevención también incluye el conocimiento por el cuerpo de
agentes que el centro de contacto es capaz de detectar cuando ha ocurrido una
actividad fraudulenta, lo que por sí mismo también proporciona un elemento
disuasorio. Además, la prevención también incluye el conocimiento por parte del
cuerpo de agentes de que el centro de contacto puede perseguir a un agente que

280 está llevando a cabo una actividad fraudulenta. Dado que la evidencia se recopila durante el proceso de monitoreo, y más específicamente cuando se detecta un posible fraude, esta evidencia se puede usar para procesar criminalmente al agente. El hecho de que la persecución penal esté sobre la mesa es un elemento disuasorio. Las implementaciones de la presente invención se hacen a lo largo de
285 este enfoque de tres puntos para tratar y prevenir el fraude dentro de un centro de contacto.

[00028] Algunas partes de las descripciones detalladas que siguen se presentan en términos de procedimientos, bloques lógicos, procesamiento y otras
290 representaciones simbólicas de operaciones sobre bits de datos dentro de una memoria de computador. Estas descripciones y representaciones son los medios utilizados por los versados en el arte de procesamiento de datos para transmitir con mayor eficacia la esencia de su trabajo a los versados en el arte. En la presente solicitud, un procedimiento, un bloque lógico, un proceso o similar, se
295 concibe como una secuencia auto-consistente de etapas o instrucciones que conducen a un resultado deseado. Las etapas son aquellas que utilizan manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas
300 y manipuladas de otro modo en un sistema de cómputo. A veces se ha demostrado conveniente, principalmente por razones de uso común, referirse a estas señales como transacciones, bits, valores, elementos, símbolos, caracteres, muestras, píxeles o similares.

305 **[00029]** Se debe tener en cuenta, sin embargo, que todos estos términos y similares se deben asociar con las cantidades físicas apropiadas y son meramente etiquetas convenientes aplicadas a estas cantidades. A menos que se indique

específicamente lo contrario como se desprende de las discusiones siguientes, se entiende que a lo largo de la presente descripción, las discusiones que utilizan
310 términos tales como "determinación", "recopilación", "captura", "referenciación cruzada" o similares, se refieren a acciones y procesos (e.g., diagramas de flujo 400 y 600 de las figuras 4 y 6) de un sistema de cómputo o dispositivo o procesador informático electrónico similar (e.g., los sistemas 100, 200 y 300 de las figuras 1-3). El sistema de cómputo o un dispositivo informático electrónico similar
315 manipula y transforma los datos representados como cantidades físicas (electrónicas) dentro de las memorias del sistema de cómputo, registros u otros tales dispositivos de almacenamiento, transmisión o visualización de información.

[00030] Las implementaciones descritas en este documento pueden ser
320 discutidas en el contexto general de instrucciones ejecutables por computador que residen en alguna forma de soporte de almacenamiento legible por computador, tales como módulos de programa, ejecutados por uno o más computadores u otros dispositivos. A modo de ejemplo, y no de limitación, los medios de almacenamiento legibles por computador pueden comprender medios de
325 almacenamiento informático no transitorios y medios de comunicación. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan determinados tipos de datos abstractos. La funcionalidad de los módulos de programa se puede combinar o distribuir según se desee en diversas
330 implementaciones.

[00031] Los medios de almacenamiento informático incluyen medios volátiles y no volátiles, removibles y no removibles implementados en cualquier método o tecnología para el almacenamiento de información tal como instrucciones legibles
335 por computador, estructuras de datos, módulos de programa u otros datos. Los

medios de almacenamiento informático incluyen, pero no se limitan a, memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), ROM programable borrrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria, disco compacto ROM (CD-ROM) Discos versátiles (DVD) u otro almacenamiento
340 óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda utilizar para almacenar la información deseada y que se pueda acceder a dicha información.

345 **[00032]** Los medios de comunicación pueden incorporar instrucciones ejecutables por computador, estructuras de datos y módulos de programa, e incluye cualquier medio de suministro de información. A modo de ejemplo, y sin limitación, los medios de comunicación incluyen medios cableados tales como una red cableada o una conexión directa por cable, y medios inalámbricos tales como
350 medios acústicos, de radiofrecuencia (RF), infrarrojos y otros medios inalámbricos. Las combinaciones de cualquiera de las anteriores también se pueden incluir dentro del alcance de los medios legibles por computador.

[00033] La figura 1 es un diagrama de bloques de un ejemplo de un sistema de
355 cómputo 100 con elque se pueden hacer implementaciones de la presente descripción. El sistema de cómputo 100 representa ampliamente cualquier dispositivo o sistema de cómputo de uno o múltiples procesadores capaz de ejecutar instrucciones legibles por computador. Ejemplos del sistema de cómputo 100 incluyen, sin limitación, estaciones de trabajo, computadores portátiles,
360 terminales del lado del cliente, servidores, sistema de cómputo distribuido, dispositivos portátiles o cualquier otro sistema o dispositivo informático. En su configuración más básica, el sistema de cómputo 100 puede incluir al menos un computador 110 y una memoria de sistema 140.

[00034] Tanto la unidad de procesamiento central (CPU) 110 como la unidad de
365 procesamiento gráfico (GPU) 120 están acopladas a la memoria 140. La memoria
de sistema 140 representa generalmente cualquier tipo o forma de dispositivo o
medio de almacenamiento volátil o no volátil capaz de almacenar datos y/u otras
instrucciones legibles por computador. Ejemplos de memoria de sistema 140
incluyen, sin limitación, memoria RAM, ROM, flash, o cualquier otro dispositivo de
370 memoria adecuado. En el ejemplo de la Fig. 1, la memoria 140 es una memoria
compartida, por lo que la memoria almacena instrucciones y datos tanto para la
CPU 110 como para la GPU 120. Alternativamente, pueden existir memorias
separadas dedicadas a la CPU 110 y la GPU 120, respectivamente. La memoria
puede incluir un búfer marco para almacenar datos de píxeles que dirigen una
375 pantalla de visualización 130.

[00035] El sistema 100 incluye una interfaz de usuario 160 que, en una
implementación, incluye un dispositivo de control de cursor en pantalla. La interfaz
de usuario puede incluir un teclado, un mouse y/o un dispositivo de pantalla táctil
380 (un touchpad).

[00036] La CPU 110 y/o GPU 120 representan generalmente cualquier tipo o
forma de unidad de procesamiento capaz de procesar datos o interpretar y
ejecutar instrucciones. En ciertas implementaciones, los procesadores 110 y/o 120
385 pueden recibir instrucciones de una aplicación de software o módulo de hardware.
Estas instrucciones pueden hacer que los procesadores 110 y/o 120 realicen las
funciones de una o más de las implementaciones de ejemplo descritas y/o
ilustradas en el presente documento. Por ejemplo, los procesadores 110 y/o 120
pueden realizar y/o ser un medio para llevar a cabo, bien sea solos o en
390 combinación con otros elementos, uno o más del monitoreo, determinación, cierre,
y detección, o similares descritos en el presente documento. Los procesadores

110 y/o 120 también pueden realizar y/o ser un medio para realizar cualquier otra etapa, método o proceso descrito y/o ilustrado en el presente documento.

395 **[00037]** En algunas implementaciones, el medio legible por computador que contiene un programa de computador se puede cargar en el sistema de cómputo 100. Todo o una parte del programa de computador almacenado en el medio legible por computador se puede almacenar entonces en la memoria de sistema 140 y/o varias partes de los dispositivos de almacenamiento. Cuando son
400 ejecutados por los procesadores 110 y/o 120, un programa de computador cargado en el sistema de cómputo 100 puede hacer que el procesador 110 y/o 120 realice y/o sea un medio para realizar las funciones de las implementaciones de ejemplo descritas y/o adicionalmente o alternativamente, las implementaciones de ejemplo descritas y/o ilustradas en el presente documento se pueden
405 implementar en firmware y/o hardware.

[00038] La FIG. 2 es una ilustración de un sistema 200 configurado para identificar la actividad fraudulenta potencial realizada por un agente dentro de un centro de contacto y tomar acción preventiva una vez que se ha identificado la
410 actividad, de acuerdo con una implementación de la presente descripción. Uno o más componentes del sistema 200 son implementables por el sistema 100 de la FIG. 1 con el fin de monitorear la actividad de agentes y/o estaciones de trabajo para identificar la actividad fraudulenta potencial y para realizar acciones adicionales una vez que se detecta la actividad, de acuerdo con una
415 implementación de la presente descripción.

[00039] El sistema 200 incluye un centro de contacto 210 que está configurado para manejar interacciones con clientes, en el que agentes del centro de contacto 210 actúan en nombre de un cliente. Por ejemplo, los agentes proporcionan

420 soporte e información a una pluralidad de clientes 270 con respecto a productos
y/o servicios asociados con el cliente. Para efectos ilustrativos únicamente, los
agentes del centro de contacto 210 pueden ayudar al cliente a completar la venta
de un producto o servicio, ayudar a un cliente a acceder a la información
gestionada por el cliente o trabajar con el cliente para manejar asuntos y
425 problemas con productos o servicios proporcionados u ofrecidos por el cliente.

[00040] La pluralidad de clientes 270 se puede comunicar con agentes en las
estaciones 230 a través de una o más redes de comunicación 250 y 280. Por
ejemplo, la red de comunicaciones 250 puede incluir un sistema de redes
430 informáticas interconectadas (e.g., Internet) que permiten la comunicación directa
entre un cliente y un cliente. Además, la red de comunicaciones 280 se puede
cualquier combinación de redes telefónicas configuradas para conectar un cliente
a un agente en una estación de trabajo particular, tal como una red de telefonía
móvil, una red telefónica pública conmutada (PSTN) basada en la línea terrestre,
435 etc.

[00041] En particular, una sección del centro de contacto 210 puede incluir una
pluralidad de estaciones de trabajo 230, que incluyen las estaciones de trabajo
230A-N. Por ejemplo, la sección puede incluir estaciones de trabajo que se
440 encuentran en varios pisos, un piso o parte de un piso del centro de contacto. La
pluralidad de estaciones de trabajo 230 es asistida por una pluralidad de agentes.
Mediante la centralización, el centro de contacto 210 puede instalar y mantener
eficientemente la infraestructura de la estación de trabajo. Además, al
proporcionar una ubicación centralizada para las estaciones de trabajo, los
445 agentes tienen fácil acceso a información, recursos y ayuda del supervisor para
proporcionar la más alta calidad de servicio a los clientes del cliente.

[00042] Una estación de trabajo se puede compartimentalizar como una unidad escalable y está configurada para proporcionar recursos esenciales que un agente
450 utiliza para gestionar solicitudes por parte de un cliente en nombre de un cliente. Por ejemplo, en parte una estación de trabajo puede incluir un sistema de cómputo (no mostrado) y un componente telefónico (no mostrado) implementado en una plataforma de trabajo.

455 [00043] El sistema de cómputo está configurado para acceder al menos a un recurso 240 de un cliente a través de una red de comunicaciones 250. Por ejemplo, el sistema de cómputo puede ejecutar una aplicación cliente que está configurada para acceder a una base de datos que contiene información relacionada con un cliente. El sistema de cómputo también puede estar
460 configurado para proporcionar comunicación entre un cliente y un agente. Por ejemplo, la comunicación puede incluir comunicaciones de voz basadas en Internet, navegación de un sitio web compartido accedido simultáneamente y conjuntamente por el cliente y el agente, comunicación basada en texto, etc.

465 [00044] El componente telefónico de una estación de trabajo está configurado para proporcionar comunicación (e.g., voz) entre un cliente y un agente que atiende a la estación de trabajo. Por ejemplo, el componente telefónico se puede acoplar a un teléfono correspondiente del cliente a través de la red de comunicaciones 280 y/o la red 250.

470 [00045] Los agentes de centros de contacto por diseño tienen acceso a información personal e identificable de clientes que son mantenidos por un cliente correspondiente. Por ejemplo, un cliente que es un banco puede almacenar información personal utilizada para identificar clientes y otra información bancaria
475 relacionada con el cliente (e.g., activos de clientes, etc.), mientras que otro cliente

(e.g., compañía de seguros, proveedor de atención médica y otros) puede tener acceso a los registros de salud de los empleados y/o clientes. Debido a que esta información (e.g., financiera y de salud) es fácilmente accesible, un agente potencialmente puede utilizar esa información para beneficio personal. Por ejemplo, un agente puede solicitar crédito utilizando información relacionada con un cliente, un agente puede comprar artículos en línea usando información de la tarjeta de crédito asociada con un cliente, o un agente puede vender información de salud personal de un cliente bien conocido.

[00046] Desafortunadamente, la actividad fraudulenta se lleva a cabo frecuentemente por agentes de un centro de contacto. Si bien la industria de centros de contacto ha reconocido esta actividad fraudulenta, la industria ha aceptado hasta ahora y absorbido las pérdidas debidas a esa actividad. Estas pérdidas pueden ser insostenibles en una era donde el robo de identidad es más frecuente y visto por el público común como inaceptable. Como tal, las implementaciones de la presente invención se pueden usar para combatir la actividad fraudulenta que se lleva a cabo por agentes de un centro de contacto. Más específicamente, las implementaciones de la presente invención son capaces de identificar y detectar cuando se está llevando a cabo la actividad fraudulenta potencial por agentes, y de tomar medidas que son capaces de remediar cualquier actividad fraudulenta y además disuadir que se cometa el fraude.

[00047] Más particularmente, la pluralidad de estaciones de trabajo 230 está configurada con una pluralidad de monitores. Es decir, cada estación de trabajo incluye un monitor que está configurado para rastrear la actividad de un sistema de cómputo correspondiente. En una implementación, el monitor está configurado dentro de un sistema de cómputo situado en la estación de trabajo correspondiente. En otra implementación, el monitor se localiza remotamente y

está configurado para recibir información recopilada desde una estación de trabajo
505 para determinar cuándo ha ocurrido una actividad fraudulenta potencial. En otra
implementación más, el monitor puede estar en una o más ubicaciones, tal como
localmente en el sistema de cómputo, y remotamente en un centro de seguridad.

[00048] Además, el sistema 200 incluye un centro de seguridad 260 que está
510 comunicativamente acoplado a la pluralidad de estaciones de trabajo 230 y está
configurado para recibir información relacionada con las actividades que están
realizando agentes sobre una pluralidad de sistema de cómputo asociados con las
estaciones de trabajo 230. En una implementación, el centro 260 de seguridad
recibe información de una pluralidad de monitores, cada uno de los cuales está
515 situado localmente en relación con una estación de trabajo correspondiente. Por
ejemplo, el recolector de información 263 del centro de seguridad 260 está
comunicativamente acoplado a cada una de las estaciones de trabajo 230A-N y
está configurado para recibir información que se puede usar para monitorear la
actividad de agentes y se puede usar para determinar cuándo se está produciendo
520 una actividad fraudulenta potencial. La información se puede almacenar en el
almacenamiento 267 para acceso posterior, tal como al realizar el análisis en la
información en un momento posterior.

[00049] En una implementación, la detección de fraude se puede realizar
525 localmente en un monitor correspondiente de una estación de trabajo, o se puede
realizar remotamente en el centro de seguridad 260, en el que la detección se
basa en la información recogida desde el monitor de la estación de trabajo
correspondiente. Por ejemplo, el centro de seguridad 260 puede incluir una unidad
de detección de fraude 262 que está configurada para detectar la actividad
530 fraudulenta potencial que está siendo realizada por un agente en una estación de
trabajo. En otra implementación, la unidad de detección de fraude 262 está situada

en una estación de trabajo, en la que la detección y las medidas posteriores tomadas se controlan localmente en esa estación de trabajo. En otras implementaciones, la detección de fraude se realiza en múltiples ubicaciones, tal como localmente en la estación de trabajo y remotamente en el centro de seguridad.

[00050] Además, se incluye un monitor de estación de trabajo o del estado de estación 264 dentro del centro de seguridad 260 y está configurado para determinar el estado de cada estación de trabajo y/o el estado del agente que atiende a dicha estación de trabajo. Por ejemplo, el monitor del estado 264 puede determinar cuándo una estación de trabajo está desconectada (e.g., la estación de trabajo está bloqueada) y cuando la estación de trabajo está en línea; puede determinar cuándo el agente está manejando una interacción o está implicado en una interacción (e.g., en una llamada) con un cliente; cuando el agente está disponible para manejar una interacción (e.g., tomar una llamada); cuando el agente está ocupado y no está disponible para manejar una interacción con un cliente (e.g., no puede recibir una llamada de un cliente); y cuando el agente está fuera almorzando. Como tal, se puede proporcionar un estado del agente y/o recursos de la estación de trabajo.

[00051] En otras implementaciones, el monitor del estado 264 es capaz de analizar y determinar estados de ánimo de agentes basados en la información recibida de los monitores en cada estación de trabajo. Por ejemplo, el monitor del estado puede determinar cuándo el agente está estresado, enojado o satisfecho.

[00052] El centro de seguridad 260 incluye un generador de mapas 265 que está configurado para identificar la pluralidad de estaciones de trabajo. Por ejemplo, el generador de mapas 265 es capaz de generar un gráfico que identifica

560 las ubicaciones de cada una de las estaciones de trabajo, y es capaz de transmitir información adicional relacionada con el estado de agentes y/o estaciones de trabajo a través de la gráfica. El gráfico generado se puede visualizar en el centro de seguridad 260 en una pantalla 266.

565 **[00053]** El centro de seguridad 260 también incluye un controlador de captura de imágenes 268. Una vez que se detecta actividad fraudulenta potencial (e.g., por la unidad de detección de fraude 262), el controlador de captura de imágenes 268 es capaz de instruir un sistema de captura de imagen 220 que está situado dentro de la sección del centro de contacto para capturar al menos una imagen de la
570 estación de trabajo que está asociada con la actividad fraudulenta potencial. Por ejemplo, el controlador de captura de imagen 268 puede retransmitir información que identifica la estación de trabajo para que el sistema de captura de imagen 220 pueda seleccionar al menos un dispositivo (e.g., una cámara de imagen o de vídeo) para orientarse a fin de capturar una vista frontal de un agente que atiende
575 a esa estación de trabajo. De esta manera, si se confirma el fraude, se puede capturar una imagen del agente que realiza el fraude. En otra implementación, el controlador de captura de imagen 268 es capaz de instruir un dispositivo de captura de imágenes situado en el sistema de cómputo de la estación de trabajo para capturar una imagen. Por ejemplo, un dispositivo de captura puede estar
580 situado en la pantalla del sistema de cómputo y es capaz de capturar una imagen de un agente que está viendo la pantalla.

[00054] Además, el centro de seguridad 260 también incluye un controlador de captura de escritorio 269. Una vez que se detecta una actividad fraudulenta
585 potencial (e.g., por la unidad de detección de fraude 262) en una estación de trabajo, el controlador de captura de escritorio 269 puede instruir al sistema de cómputo en la estación de trabajo y/o al monitor en la estación de trabajo para

capturar una o más imágenes de escritorio del sistema de cómputo. Por ejemplo, las imágenes se recogen durante un periodo de tiempo suficiente para determinar si la actividad fraudulenta fue efectivamente realizada por un agente en la estación de trabajo correspondiente. De esta manera, si se confirma el fraude, una o más imágenes del fraude que se realiza usando el sistema de cómputo se pueden capturar como evidencia. La evidencia se puede usar para probar el fraude, y esa evidencia se puede usada al terminar y/o enjuiciar al agente en cortes criminales y/o civiles.

[00055] La FIG. 3 es un diagrama de bloques de componentes de una estación de trabajo del centro de contacto 300 que están configurados para monitorear la actividad de un agente del centro de contacto con el fin de identificar la actividad fraudulenta potencial realizada por el agente, de acuerdo con una implementación de la presente descripción. La estación de trabajo 300 se puede implementar por el sistema 100 de la FIG. 1 con el fin de monitorear la actividad de un agente y/o estación de trabajo correspondiente para identificar la actividad fraudulenta potencial y para realizar acciones adicionales una vez que se detecta la actividad, de acuerdo con una implementación de la presente descripción. Además, la estación de trabajo 300 es representativa de las estaciones de trabajo 230A-N en la FIG. 2.

[00056] La estación de trabajo 300 está configurada para permitir el monitoreo en tiempo real, la detección de fraude y la prevención del fraude, tal como se hace a través de las implementaciones de la presente invención. Por ejemplo, diferentes componentes de la estación de trabajo 300 operan conjuntamente para rastrear la actividad del agente con el fin de detectar y documentar la actividad fraudulenta, y para tomar medidas subsiguientes para prevenir futuros fraudes.

615

[0057] Como se ha descrito anteriormente, cada estación de trabajo en un centro de contacto puede estar organizada como una unidad escalable y contiene componentes esenciales para permitir que un agente asistente se comuniquen con un cliente y proporcione servicios a ese cliente en nombre de un cliente. Por ejemplo, el recurso de comunicación 320 permite que el agente se comuniquen con el cliente, y puede incluir un teléfono u otro dispositivo con base en voz o texto. Además, la estación de trabajo 300 incluye un recurso de cálculo multipropósito 310. En una implementación, el recurso de cómputo 310 está configurado para acceso a los recursos del cliente. Por ejemplo, al tratar o involucrarse en una interacción con un cliente (e.g., manejar una llamada de un cliente), el agente que actúa en nombre del cliente y a través del recurso de cómputo 310 tiene acceso a recursos basados en el cliente (e.g., aplicaciones, bases de datos, etc.) que contienen información personal e identificable relacionada con el cliente. Además, el recurso de cómputo 310 puede estar configurado para permitir la comunicación primaria o de soporte con un cliente. Por ejemplo, el recurso 310 se puede usar para permitir o facilitar el acceso simultáneo de un sitio web por el cliente y el agente. Además, las capacidades del recurso de cómputo 310 se pueden utilizar para implementar el seguimiento de la actividad del agente en el recurso de cómputo 310, la detección de fraude y/o la prevención del fraude independientemente o conjuntamente con otros componentes en la estación de trabajo 300 o componentes o dispositivos situados remotamente (e.g., situado en un centro de seguridad).

[0058] La estación de trabajo 300 también incluye una unidad de monitoreo 330, que está configurada para rastrear la actividad de los componentes dentro de la estación de trabajo 300 y/o la actividad del agente correspondiente solo o en conjunción con dichos componentes. En las implementaciones, la unidad de monitoreo 330 se puede ser una unidad autónoma o se puede incluir dentro del

recurso de cómputo 320. Por ejemplo, la unidad de monitoreo 330 se puede
645 configurar para rastrear la actividad realizada sobre el recurso de comunicación
320, de tal manera que se pueda generar un registro de uso que indique en qué
momentos el recurso de comunicación 320 estaba en uso, presumiblemente por
un agente correspondiente y esperado. La unidad de monitoreo 330 también es
capaz de grabar conversaciones mantenidas a través del recurso de comunicación
650 320. De esta manera, la unidad de monitoreo 330 puede realizar un seguimiento
cuando el recurso de cómputo 310 inicia sesión y se desconecta del centro de
contacto y/o de los recursos en una estación de trabajo correspondiente, cuando
el recurso de cómputo 310 está ejecutando una aplicación de un cliente, cuando el
recurso de cómputo 310 está accediendo a un recurso particular del cliente y
655 cualquier otra actividad cuantificable que se realiza en el recurso de cómputo 310.

[00059] Además, la unidad de monitoreo 330 es capaz de rastrear el estado de
un agente asistente en la estación de trabajo 300 con base en la entrada
proporcionada al recurso de cómputo 310 por el agente. Por ejemplo, la unidad de
660 monitoreo 330 es capaz de determinar la disponibilidad del agente asistente sobre
la base del estado de inicio de sesión del recurso de cómputo 310. En otros casos,
la unidad de monitoreo 330 es capaz de rastrear cuándo el agente está en una
pausa o fuera almorzando, con base en el historial de actividad del recurso de
cómputo 310, o con base en el estado de inicio de sesión proporcionado por el
665 agente al recurso 310.

[00060] Además, la unidad de monitoreo 330 es capaz de rastrear el estado
emocional del agente. Por ejemplo, con base en la evidencia de apoyo recogida
directamente por el monitor 330, se puede hacer una inferencia sobre el estado
670 emocional del agente. Como ilustración, las expresiones faciales, el nivel de
volumen, la frecuencia de hablar, la frecuencia cardíaca, otras mediciones

biométricas, etc., se pueden usar para determinar el estado emocional de un agente.

675 **[00061]** Con base en la información recogida por la unidad de monitoreo 330, se puede realizar un análisis adicional. Por ejemplo, la información recolectada de una o más estaciones de trabajo se puede usar para establecer una línea de base de la actividad del agente específico para un agente individual, o para los agentes tratados como un grupo. Las ilustraciones de los datos de la línea de base
680 incluyen el tiempo promedio que maneja o está implicado en una interacción con un cliente, tiempo promedio que asiste a un cliente en una llamada, tiempo promedio que accede a un recurso del cliente, el número de veces que un recurso del cliente se accede, el tiempo que un agente ha colocado al cliente en espera, etc. Esta información se puede usar para calificar el desempeño de un cliente en
685 particular con base en una comparación con el promedio estadístico. Esta información también se puede usar para determinar si se ha producido una actividad fraudulenta potencial, como cuando la actividad del agente cae fuera de la norma estadística, como se describirá más detalladamente a continuación.

690 **[00062]** La estación de trabajo 300 opcionalmente incluye una unidad de detección de fraude 340. Con base en la información recogida por la unidad de monitoreo 330, la unidad de detección de fraude 340 puede determinar cuándo ciertas actividades o combinación de actividades realizadas sobre o por los componentes de la estación de trabajo 300 y/o el agente asistente indica que el
695 agente está realizando actividades potencialmente fraudulentas. Por ejemplo, según se determina por la unidad de detección de fraude 340, la información recogida puede coincidir con ciertas reglas o patrones de actividades que se sabe que ocurren cuando se realiza un fraude. En otros casos, se puede detectar actividad fraudulenta potencial cuando la actividad del agente cae fuera de la

700 norma estadística de un grupo de agentes o de ese agente particular. Como tal, la
unidad de detección 340 puede proporcionar una notificación de que se está
llevando a cabo una actividad fraudulenta potencial en la estación de trabajo 300
por un agente. Por ejemplo, la notificación se puede proporcionar a través de un
gráfico del centro de contacto.

705

[00063] El análisis realizado para detectar actividad fraudulenta potencial se
puede realizar por una unidad de detección de fraude local 340, una unidad de
detección de fraude remoto (e.g., situada en un centro de seguridad) o una
combinación de las unidades de detección de fraude locales y remotas. Además,
710 la detección de un posible fraude puede ocurrir en tiempo real, o después de que
se haya producido la actividad fraudulenta potencial, como durante un período de
análisis post-ocurrencia.

[00064] La estación de trabajo 300 incluye un dispositivo de captura de
715 imágenes 350. Una vez que se ha detectado una actividad fraudulenta potencial
por la unidad 340, el dispositivo de captura de imagen 350 se puede activado
visualmente, registrar la actividad por el agente en la estación de trabajo. Por
ejemplo, el dispositivo de captura de imágenes 350 puede estar integrado con una
pantalla e instruido para capturar una vista facial del agente. De esta manera, se
720 recoge una imagen del agente que lleva a cabo la actividad fraudulenta potencial
para identificar el agente, y también se guarda como evidencia. La información
adicional (e.g., información de inicio de sesión, biometría de inicio de sesión,
biometría, etc.) se puede referenciar de forma cruzada para verificar la identidad
del agente cuya imagen facial se captura. El dispositivo de captura de imágenes
725 350 de la estación de trabajo 300 puede trabajar conjuntamente con un sistema de
captura de imágenes del centro de contacto que tiene dispositivos de captura

localizados en todo el centro de contacto, tal como en estaciones de trabajo y/o más generalmente situados en y alrededor de un piso de un centro de contacto.

730 **[00065]** La estación de trabajo 300 incluye un dispositivo de captura de escritorio 360. Una vez que se ha detectado una actividad fraudulenta potencial por la unidad 340, el dispositivo de captura de escritorio 360 se puede activar para recoger una o más imágenes del escritorio según lo ve el agente en la pantalla asociada con el recurso de cómputo 310. El dispositivo de captura de escritorio
735 360 puede estar integrado o independiente del recurso de cómputo 310. De esta manera, una o más imágenes del escritorio mientras se está realizando un fraude se pueden capturar como evidencia y utilizar cuando se termina y/o enjuicia al agente en los tribunales penales o civiles. Uno o más dispositivos en todo el sistema están orientados (e.g., ajustar al zoom) para capturar una vista frontal de
740 un agente que lleva a cabo la actividad fraudulenta potencial. Como se describió anteriormente, también se puede recopilar información adicional de los recursos disponibles para un agente en una estación de trabajo que puede o no se puede presentar en un escritorio. Esta información se puede recoger utilizando el dispositivo de captura de escritorio 360 y/o un dispositivo de monitoreo asociado.
745 Por ejemplo, se registra la dirección de protocolo de Internet (IP) de un recurso de cliente al que accede el agente, las marcas de tiempo de cuando el agente está utilizando un recurso de estación de trabajo, etc.

[00066] Aunque se describen implementaciones de la presente invención dentro
750 del contexto de la detección de actividad fraudulenta potencial en tiempo real, los métodos descritos en los diagramas de flujo 400 y 600 de las Figs. 4 y 6 son adecuados para la detección de actividad potencialmente fraudulenta después de que ocurra. Por ejemplo, la información relacionada con la actividad del agente durante un período de 24 horas se puede entregar a un centro de seguridad para

755 el análisis de detección de fraude. Una vez que se ha detectado una actividad fraudulenta potencial, se puede llevar a cabo una investigación adicional utilizando la información recopilada o supervisando de cerca la actividad de un agente sospechoso en el futuro.

760 [00067] La FIG. 4 es un diagrama de flujo 400 que ilustra un método para detectar actividad fraudulenta potencial y tomar medidas preventivas una vez que se detecta la actividad fraudulenta, de acuerdo con una implementación de la presente descripción. En otra implementación más, el diagrama de flujo 400 ilustra un método implementado por computador para detectar actividad fraudulenta
765 potencial y tomar medidas preventivas una vez que se detecta la actividad fraudulenta. En otra implementación, el diagrama de flujo 400 se implementa en parte dentro de un sistema de detección de fraude que incluye un procesador de computador y una memoria acoplada al procesador y que tiene almacenadas en ella instrucciones que, si son ejecutadas por el sistema de cómputo hace que el
770 sistema ejecute un método para detectar actividad fraudulenta potencial y tomar medidas preventivas una vez que se detecta la actividad fraudulenta. En otra implementación más, las instrucciones para llevar a cabo un método como se describe en el diagrama de flujo 400 se almacenan en un medio de almacenamiento no transitorio legible por computador que tiene instrucciones
775 ejecutables por computador para hacer que un sistema de cómputo realice un método para detectar actividad fraudulenta potencial y tomar medidas preventivas una vez detectada la actividad fraudulenta. En las implementaciones, el método esbozado en el diagrama de flujo 400 se puede implementar por uno o más componentes de los sistemas 100, 200, 300 y 500A de las Figs. 1-3 y 5,
780 respectivamente.

[00068] En 410, el método incluye determinar que se está llevando a cabo una actividad fraudulenta potencial en un centro de contacto, en el que el centro de contacto comprende una pluralidad de estaciones de trabajo atendidos por una pluralidad de agentes. Por ejemplo, el centro de contacto se puede representar del centro de contacto 200 de la FIG. 2.

[00069] El método incluye el control de una pluralidad de agentes en un centro de contacto que comprende una pluralidad de estaciones de trabajo. Cada uno de la pluralidad de agentes está asignado a una de la pluralidad de estaciones de trabajo. Por ejemplo, el centro de contacto se puede configurar para manejar las interacciones con los clientes mientras representa un cliente. Por ejemplo, el centro de contacto puede estar configurado para gestionar llamadas para un cliente (e.g., banco, almacén por departamentos, etc.) y, como tal, la pluralidad de agentes puede manejar una pluralidad de llamadas entrantes y salientes. Como se ha descrito anteriormente, el monitoreo permite la recopilación de información relacionada con las actividades de los agentes y/o actividades que se realizan en los recursos utilizados por los agentes. En una implementación, se lleva a cabo el monitoreo de la actividad electrónica de los agentes (e.g., actividad de la computadora, actividad del teléfono, etc.). Además, la información monitoreada se puede recoger en un lugar centralizado para su almacenamiento y análisis. En una implementación, el método incluye monitorear un primer agente en una primera estación de trabajo y, en particular, monitorear las interacciones del agente con los recursos (e.g., recurso de cómputo) de la estación de trabajo. Además, se puede monitorear la interacción del agente con un recurso del cliente. Por ejemplo, se controla la interacción con una base de datos de clientes. Además, la interacción del agente con el sistema de comunicación se monitorea para determinar cuándo el agente está manejando o está involucrado en una interacción (e.g., en una

llamada) y si el agente está disponible para ayudar a un nuevo cliente a través de
810 otra interacción (e.g., tomar otra llamada).

[00070] En una implementación, el monitoreo es continuo, en la que el
monitoreo se realiza cuando el agente está manipulando o está implicado en una
interacción (e.g., manejando llamadas) y cuando el agente no está manipulando o
815 no está implicado en una interacción. Es decir, se controla toda la actividad del
agente y/o las actividades que se realizan en los recursos de la estación de
trabajo. En otras implementaciones, el monitoreo es periódico o se realiza de
forma aleatoria. Por ejemplo, sólo se necesita una muestra estadística para
determinar la actividad fraudulenta, y en lugar de desperdiciar recursos, el
820 monitoreo se realiza sobre una base menos que continua.

[00071] Se pueden implementar diversas técnicas para determinar que la
actividad de un agente es potencialmente fraudulenta y que requiere mayor
atención. Por ejemplo, en una implementación, un agente puede estar implicado
825 en actividad sospechosa que es generalmente indicativa de actividad fraudulenta.
En particular, cuando un agente está accediendo a información personal e
identificable (e.g., a través de una base de datos de clientes) relacionada con un
cliente de un cliente, pero no está ayudando al cliente (e.g., no en una llamada con
el cliente), entonces esa actividad es sospechosa. Esta actividad se puede
830 identificar como coincidente con los criterios y conducir a una determinación de
que la actividad fraudulenta potencial puede haber sido realizada por el agente. Se
puede necesaria una investigación adicional para determinar si se ha producido un
fraude real. Por otra parte, si el monitoreo determina que el agente posicionado
está accediendo a una base de datos de cliente para información del cliente y que
835 el agente está actualmente ayudando a ese cliente en relación con la información
accedida, se autoriza la actividad y el acceso a la base de datos del cliente. La

FIG. 6 proporciona una discusión detallada sobre la detección de una actividad fraudulenta potencial que coincide con un cierto conjunto de criterios.

840 **[00072]** La determinación de que se ha producido una actividad fraudulenta potencial se puede realizar en un centro de seguridad que está centralizado a una pluralidad de estaciones de trabajo de un centro de contacto. En particular, el centro de seguridad está configurado para recibir una pluralidad de información relacionada con las actividades de agentes y/o actividades que se realizan en
845 recursos de la pluralidad de estaciones de trabajo. Esa información, recogida en cada una de las estaciones de trabajo, luego es entregada a través de una red de comunicación al centro de seguridad para un análisis posterior, y más específicamente para determinar cuándo ha ocurrido una actividad fraudulenta potencial.

850

[00073] Por ejemplo, la determinación de que se ha producido una actividad fraudulenta potencial se basa en si la información relativa a actividades de un agente y/o actividades que se realizan sobre recursos de una estación de trabajo viola cualquier regla predefinida o predeterminada. Las reglas se pueden definir
855 por uno o más parámetros y/o criterios. Más particularmente, se puede determinar que se ha producido una actividad fraudulenta potencial cuando la información indica una violación de una regla. Como ilustración, la regla puede definir una línea de base de transacciones, acciones o actividades realizadas por uno o más agentes junto con el uso de recursos de estaciones de trabajo (e.g., teléfono,
860 recursos informáticos, etc.). Por ejemplo, la línea de base puede estar definida por un promedio estadístico en relación con una actividad asociada con el agente y/o la pluralidad de agentes. Además, la línea de base puede estar dirigida o corresponder a al menos una primera actividad. Por ejemplo, la línea de base puede describir el número promedio de llamadas salientes realizadas por agentes

865 durante un período de tiempo predefinido (e.g., 1 hora, 2 horas, turno diario, etc.). En otro ejemplo, la línea base puede describir el número de veces que un agente coloca a los clientes en espera durante un período y/o la duración del tiempo de espera cada vez que un cliente se pone en espera. Una condición atípica que es realizada por un agente se puede monitorear y descubrir, cuando la condición

870 atípica se encuentra fuera de la línea de base. Es decir, lo atípico muestra patrones inusuales de actividad. Si la condición atípica satisface la regla (e.g., parámetros y/o criterios), entonces se puede determinar que se ha producido una actividad fraudulenta potencial. Además, la condición externa puede coincidir con una actividad fraudulenta conocida que está asociada con la regla. Debido a que

875 los valores atípicos pueden ocurrir de vez en cuando, inusualmente los números altos de valores atípicos se puede una indicación de fraude. Es necesaria una investigación adicional para determinar si existe fraude real.

[00075] En un ejemplo, la actividad de fraude potencial por un agente ocurre

880 cuando hay tiempos excesivos de retención de llamada, cuando se compara con un promedio estadístico de una pluralidad de agentes en el centro de contacto. Un agente que es registrado por tener tiempos de espera excesivos, puede estar tratando de acceder fraudulentamente a información personal e identificable mientras tiene una llamada telefónica activa con un cliente. En este escenario, en

885 un esfuerzo por vencer una solución antifraude, el agente del centro de contacto podría poner en espera un cliente de teléfono válido y luego acceder a la información personal e identificable de otro cliente.

[00075] En otro ejemplo más, la actividad fraudulenta potencial por un agente se

890 produce cuando un agente genera una llamada saliente en un momento que es incongruente con las acciones de otros agentes. Es decir, el patrón típico de los agentes en el centro de contacto muestra que los agentes están manejando

llamadas entrantes. Otro patrón puede mostrar que el agente individual durante un período histórico sólo ha manejado llamadas entrantes. El agente del centro de
895 contacto podría tratar de superar una solución antifraude estableciendo una Falsa "llamada telefónica" simplemente haciendo una llamada saliente, y luego acceder fraudulentamente a la información personal e identificable del cliente.

[00076] En otro ejemplo, la actividad fraudulenta potencial por un agente ocurre
900 cuando un agente está accediendo a formas y exhibe características fuera de un promedio estadístico incluyendo acciones de otros agentes o ese agente particular. Por ejemplo, la duración del agente dentro de las formas o páginas identificadas de la aplicación se compara con la línea de base normal con base en promedios estadísticos de todos los agentes del centro de contacto para
905 determinar cualquier desviación.

[00077] En 420, el método incluye determinar que la actividad fraudulenta potencial tiene lugar en una primera estación de trabajo. En particular, la identidad de la estación de trabajo es importante a efectos de identificar qué agente o
910 individuo está realizando la actividad. La identidad de la estación de trabajo se determina a partir de la información utilizada para determinar que se ha producido una actividad fraudulenta potencial. Por ejemplo, la información de identificación de un recurso informático sobre el cual se ha producido la actividad puede estar referenciada en cruz para determinar la estación de trabajo correspondiente dentro
915 de la cual se realizó la actividad. Una vez identificada, se puede recopilar información adicional relacionada con la estación de trabajo, como determinar el agente que está programado para trabajar en el momento en que ocurrió la actividad fraudulenta potencial.

920 **[00078]** En 430, el método incluye proporcionar una notificación de evento de la actividad fraudulenta potencial. La notificación de eventos puede incluir la información utilizada para determinar que se ha producido una actividad fraudulenta potencial y puede incluir información que identifique la estación de trabajo y cualquier información adicional que identifique al agente involucrado en la actividad. Por ejemplo, la notificación se puede proporcionar a un especialista en seguridad (e.g., un analista de riesgos) ubicado en un centro de seguridad. El especialista en seguridad está capacitado para analizar la información recopilada indicando que se ha producido una actividad fraudulenta potencial y para llevar a cabo investigaciones adicionales para determinar si se realizó un fraude real. El

930 especialista en seguridad puede realizar un monitoreo adicional para determinar si el agente está de hecho realizando acciones fraudulentas. Por ejemplo, el especialista en seguridad puede monitorear la actividad del agente y/o los recursos de la estación de trabajo durante un período de tiempo para determinar si la actividad previamente identificada es fraudulenta o si el agente está llevando a

935 cabo actividades fraudulentas. La revisión de la actividad y/o evidencia del agente en relación con una notificación de evento de actividad fraudulenta potencial por parte del especialista de seguridad puede ocurrir casi en tiempo real o en un momento posterior en relación con la ocurrencia de la actividad fraudulenta potencial. Es decir, la actividad del agente, así como cualquier desencadenador

940 (e.g., notificación de evento, violaciones de normas, etc.) de la actividad fraudulenta potencial se almacena y se accede en un momento posterior para el análisis. En otras implementaciones, el monitoreo adicional se puede realizado automáticamente por un sistema de monitoreo.

945 **[00079]** En una implementación, la notificación de evento se proporciona en un mapa o gráfico del centro de contacto, en el que el gráfico identifica una pluralidad de estaciones de trabajo y/o proporciona información del estado para cada

estación de trabajo. Por ejemplo, el gráfico puede indicar las ubicaciones de cada estación de trabajo. Por ejemplo, el gráfico puede ilustrar una sección de un centro de contacto e incluir las ubicaciones de las estaciones de trabajo a lo largo de la distribución del piso de un piso del edificio. De esta manera, cada estación de trabajo de la sección del centro de contacto está representada en el mapa.

[00080] Además, las estaciones de trabajo pueden estar representadas cada una por uno o más iconos. Un icono puede reflejar la información del estado de la estación de trabajo y/o el agente programado para atender la estación de trabajo. La información del estado se basa en la información relacionada con la actividad del agente y/o actividad que se está realizando en los recursos de la estación de trabajo que se reciben de cada una de las estaciones de trabajo. Por ejemplo, la información del estado puede incluir si el agente está conectado o desconectado del sistema del centro de contacto, si el agente está manejando o está involucrado en una interacción, si el agente está en una llamada, si el agente está fuera almorzando, si el agente está disponible para tomar una llamada, si el agente está disponible para manejar otra interacción con otro cliente, etc. Además, los iconos en la carta pueden indicar si hay actividad fraudulenta potencial que se está llevando a cabo en la estación de trabajo o si la actividad fraudulenta potencial se llevó a cabo en el pasado en la estación de trabajo. Se proporciona una descripción más detallada de los iconos del centro de contacto y de la estación de trabajo en relación con las Figs. 7A-K, a continuación.

[00081] En 440, el método incluye capturar al menos una imagen de la primera estación de trabajo. Esta información se puede recolectar para evidencia adicional que demuestre fraude, y también más particularmente se recoge con el propósito de identificar al agente que está relacionado con la determinación de la actividad fraudulenta potencial (i.e., el agente que potencialmente comete fraude). Por

ejemplo, al menos una trama de imagen captura una vista frontal de la primera estación de trabajo y, más particularmente, una vista frontal del agente que atiende a la primera estación de trabajo. Esto puede incluir apuntar al menos un dispositivo de captura de imágenes (e.g., cámara) en la primera estación de trabajo. Por ejemplo, un dispositivo de captura de imágenes puede realizar una serie de operaciones con el fin de capturar la(s) imagen(es) correspondiente(s). Las operaciones incluyen panoramizar el dispositivo en una dirección para que el dispositivo sea capaz de ver la primera estación de trabajo. Además, el dispositivo de captura de imagen se titula en un ángulo de modo que el dispositivo sea capaz de ver la primera estación de trabajo. Mientras que en este punto, una imagen capturada incluirá la estación de trabajo, la ampliación puede ser demasiado pequeña para mostrar información relevante y, como tal, las operaciones pueden incluir ampliar el dispositivo de captura de imágenes a una ampliación mayor para obtener una vista ampliada de la estación de trabajo y/o del agente que atiende a la primera estación de trabajo.

[00082] En una implementación, el método incluye determinar una identidad de un agente posicionado que asiste a la primera estación de trabajo, y almacenar esa identidad. Esto se logra capturando información de identificación del agente posicionado. Por ejemplo, la al menos una imagen que se captura se puede utilizar con fines de identificación. Específicamente, la primera información de identificación puede incluir una imagen facial del agente posicionado. Se puede recoger información adicional para determinar positivamente la identidad del agente posicionado. Por ejemplo, se puede determinar una segunda información de identificación que se asocia con un agente programado para atender la estación de trabajo y se asigna a la estación de trabajo en el momento en que se produjo la actividad potencialmente fraudulenta. En particular, se accede a un registro desde una base de datos de empleados de un cliente, en el que el registro

corresponde al agente programado. Como tal, el registro puede incluir información
1005 que detalle el nombre del agente programado, una imagen fotográfica del agente,
el departamento dentro del cual ese agente trabaja, el número de identificación del
empleado y otra información de identificación.

[00083] En algunas implementaciones, la segunda información de identificación
1010 se determina a partir de la información obtenida además de la información de
registro del empleado. Esto puede proporcionar información de soporte utilizada
para verificar la identidad del agente posicionado. Por ejemplo, en lugar de utilizar
información relacionada con un agente programado, se puede utilizar información
de inicio de sesión para un agente asistente. Es decir, la información biométrica de
1015 un agente (e.g., el agente que atiende a la estación de trabajo) se captura durante
un proceso de inicio de sesión en la primera estación de trabajo y se hace
referencia cruzada con información biométrica conocida almacenada en registros
de empleados de la pluralidad de agentes para determinar la identidad del agente
asistente, en el que los registros del empleado se pueden almacenar en una base
1020 de datos del cliente. El proceso de inicio de sesión puede haberse realizado antes
del momento en que se produjo la actividad fraudulenta potencial y, como tal, el
agente asistente puede no estar posicionado, puede estar cometiendo la actividad
potencialmente fraudulenta mientras actúa como agente asistente. Como
ilustración, se puede recoger una huella dactilar del agente asistente, se puede
1025 recopilar información del ojo del agente y cualquier otro dato biológico se puede
utilizar para identificar un agente que supuestamente está asignado a la estación
de trabajo y/o atender el puesto de trabajo. Se puede usar otra información, tal
como el nombre de inicio de sesión que es autenticado por el agente (e.g., a
través de una contraseña).

1030

[00084] Posteriormente, la primera información de identificación (e.g., imagen capturada) y la segunda información de identificación (e.g., información de registro de empleado, información biométrica, etc.) se pueden hacer referencia cruzada adicional para identificar el agente posicionado. Específicamente, la imagen facial del agente posicionado se hace referencia cruzada con la información de registro de empleado (e.g., foto de empleado) del agente programado, o el agente asistente identificado a través del proceso de inicio de sesión. Por ejemplo, la imagen del agente posicionado se compara con una imagen del agente programado y/o el agente asistente previamente determinado. Si hay una coincidencia, el agente posicionado se verifica y se autentica como el agente programado y/o el agente asistente.

[00085] Por otra parte, si la imagen facial del agente posicionado no coincide con la información de registro relacionada con el agente programado o asistente, entonces el método determina que el agente posicionado no es el agente programado y se puede realizar operaciones adicionales para identificar el agente posicionado. Por ejemplo, se pueden realizar técnicas de reconocimiento facial en la imagen facial y se hace referencia cruzada con información en cada uno de los registros del empleado para que coincida el agente posicionado con un registro de empleado. Además, se puede proporcionar una notificación adicional indicando que la actividad fraudulenta potencial está siendo realizada por un agente no programado. Esta notificación se puede proporcionar al centro de seguridad, al especialista de seguridad en el centro de seguridad y/o se puede proporcionar actualizando la información del estado dentro de un gráfico del centro de contacto (e.g., un icono que indica dicha notificación).

[00086] La FIG. 5A es un diagrama que ilustra un piso del centro de contacto 500A que incluye una pluralidad de estaciones de trabajo y un sistema de captura

de imágenes 550 (e.g., un sistema de monitoreo de cámara o video) configurado para ver cada una de las estaciones de trabajo, de acuerdo con una implementación de la presente descripción. Una pluralidad de estaciones de trabajo 510 está organizada a lo largo del piso 500A del centro de contacto. Como se muestra, las estaciones de trabajo 510A-N están diseminadas a través de un suelo de edificio 500A del centro de contacto.

[00087] Más específicamente, el sistema de captura de imágenes 550 puede incluir uno o más dispositivos de captura de imágenes 550A-N. Por ejemplo, el sistema 550 puede incluir dispositivos montados en la pared o en el techo que son capaces de ver múltiples estaciones de trabajo. Además, el sistema de captura de imágenes 550 puede incluir dispositivos de captura de imágenes que están configurados para capturar imágenes de una única estación de trabajo, tal como un dispositivo que está integrado dentro de una pantalla de visualización de un recurso de cómputo en una estación de trabajo correspondiente (no mostrada). Como tal, se puede activar un dispositivo de captura de imagen apropiado e instruirse para capturar al menos una imagen de una estación de trabajo correspondiente donde se está produciendo actividad potencialmente fraudulenta y/o al menos una imagen del agente posicionado que comete la actividad potencialmente fraudulenta.

[00088] En la Fig. 5A, cada uno de los dispositivos de captura de imágenes 550A-N es controlable para orientarse a una estación de trabajo seleccionada, por ejemplo, una estación de trabajo en la que se está produciendo actividad potencialmente fraudulenta. Una vez identificada la estación de trabajo objetivo, se instruye al menos un dispositivo de captura de imagen en el sistema de captura de imágenes 550 para orientarse de modo que tenga una vista de la estación de trabajo objetivo.

[00089] La FIG. 5B es un diagrama que ilustra una disposición típica de los recursos disponibles para una estación de trabajo del centro de contacto 510A de las Figs. 5A-B y un dispositivo de captura de imágenes 550A configurado y orientado para capturar una vista frontal de un agente posicionado que asiste a la estación de trabajo. Como se muestra, la estación de trabajo 510A incluye un recurso de computo 530 (e.g., sistema de cómputo y teclado) utilizado para la comunicación y/o acceso a recursos de cliente, y un recurso de comunicación 540 (e.g., auricular telefónico o de audio) utilizado para comunicar con un cliente de un cliente. Tanto el recurso de cómputo 530 como el recurso de comunicación 540 se pueden colocar encima de una plataforma de trabajo 520 (e.g., un escritorio). Un agente posicionado se sienta en la silla 550 cuando se utiliza el recurso de computo 520, tal como al realizar una actividad potencialmente fraudulenta. Como tal, la estación de trabajo 510A esta compartimentalizada como una unidad para proporcionar todo lo que un agente de servicio necesita en una cantidad mínima de espacio. En muchos casos, el computador del agente está acoplado a una red informática que proporciona, entre otros, recursos de fondo, computadores virtuales, bases de datos informativas, una ruta de comunicación con un supervisor inmediato, conexión a otros centros de contacto o un protocolo de enrutamiento para interacción con un cliente (e.g., una llamada) a un agente o división más apropiados.

[00090] Como se muestra en las Figs. 5A-B, el dispositivo de captura de imágenes 550A está configurado para tener una vista de la estación de trabajo objetivo 510A. Por ejemplo, cuando está orientado correctamente, el dispositivo de captura de imágenes 550A tiene un campo de visión 560 que incluye la estación de trabajo 510A. Como tal, el dispositivo de captura de imágenes 550A puede instruirse para capturar al menos una imagen de la estación de trabajo y/o agente posicionado simultáneamente con o en asociación con la detección de actividad

1115 potencialmente fraudulenta que ocurre en la estación de trabajo 510A, de acuerdo con una implementación de la presente descripción. Como tal, el dispositivo de captura de imágenes 550A se puede activar y orientar (e.g., ajustar al zoom) de modo que tenga una vista ampliada de la estación de trabajo 510A y/o del agente posicionado que asiste a la estación de trabajo 510A.

1120

[00091] La FIG. 6 es un diagrama de flujo 600 que ilustra un método para realizar detección de fraude, tal como en un centro de contacto, de acuerdo con una implementación de la presente descripción. En otra implementación más, el diagrama de flujo 600 ilustra un método implementado por computador para

1125 realizar la detección de fraude, tal como en un centro de contacto. En otra implementación, el diagrama de flujo 600 se implementa en parte dentro de un sistema de detección de fraude que incluye un procesador de un computador y una memoria acoplada al procesador y que tiene almacenadas en ella instrucciones que, si son ejecutadas por el sistema de cómputo hace que el

1130 sistema ejecute un método para realizar detección de fraude, como en un centro de contacto. En otra implementación más, las instrucciones para llevar a cabo un método como se describe en el diagrama de flujo 600 se almacenan en un medio de almacenamiento no transitorio legible por computador que tiene instrucciones ejecutables por computador para hacer que un sistema de cómputo realice un

1135 método para ejecutar la detección de fraude, tal como en un centro de contacto. En las implementaciones, el método esbozado en el diagrama de flujo 600 se puede implementar por uno o más componentes de los sistemas 100, 200, 300, 500A de las Figs. 1-3 y 5, respectivamente.

1140 [00092] Aunque los agentes del centro de contacto tienen inherentemente acceso a la información de identificación personal de los clientes a través de recursos basados en el cliente, estos agentes sólo deben usar este acceso según

una necesidad de acceso. Por ejemplo, el acceso se puede autorizar cuando un agente está manejando o está involucrado en una interacción, tal como
1145 manejando una llamada y llevando a cabo una conversación con un cliente en el teléfono. En otro ejemplo, el acceso está autorizado cuando el agente tiene una razón válida para acceder a los datos cuando no está involucrado en una interacción con un cliente (manejar una llamada), como cuando el agente está revisando la cuenta del cliente para fines de garantía de calidad. Las
1150 implementaciones de la presente invención, tal como se describen en el diagrama de flujo 600, se utilizan para identificar cuando un agente está en violación de un conjunto particular de criterios, es decir, cuando accede a recursos del cliente cuando no participa en una interacción (e.g., en una llamada) con un cliente.

1155 **[00093]** En 610, el método incluye determinar que un primer agente en una primera estación de trabajo de un centro de contacto no está manejando una interacción o no participa en una interacción con un cliente (e.g., en una llamada) en una primera vez. Como se ha descrito anteriormente, el centro de contacto incluye una pluralidad de estaciones de trabajo atendidos por una pluralidad de
1160 agentes. Las actividades de cada agente, incluyendo las interacciones con los recursos de la estación de trabajo, así como el rendimiento de los recursos de la estación de trabajo, se monitorean, como se describió anteriormente. De esta manera, a través del monitoreo, se conoce la actividad del agente, incluyendo si el agente está actualmente involucrado en una interacción con un cliente, manejando
1165 una llamada, está disponible para manejar una interacción, está disponible para manejar una llamada, está fuera almorzando, se inicia o se termina una sesión, etc.

[00094] En un caso, cuando el agente no está implicado en una interacción
1170 (e.g., en una llamada), el agente puede estar disponible para manejar una

interacción (e.g., tomar una llamada) con un cliente del cliente u otro cliente (e.g., cuando el agente está manejando interacciones (e.g., llamadas) con múltiples clientes). En otro caso, el agente puede estar en el almuerzo. Es decir, el agente ha introducido activamente su estado en el recurso de cómputo en la estación de trabajo para indicar que el agente está tomando un descanso y, más específicamente, una pausa para el almuerzo. Todavía se contemplan otros ejemplos para cuando el agente no maneja una interacción con un cliente (e.g., en una llamada).

[00095] También, en 620, el método incluye determinar que el primer agente está accediendo a un recurso con base en el cliente en la primera vez. El recurso está asociado con un cliente. Una vez más, esta determinación se hace a través del monitoreo del agente y/o de las actividades realizadas sobre los recursos de la estación de trabajo. Como se ha descrito anteriormente, el recurso puede ser una base de datos que contiene información personal e identificable de empleados, clientes, socios, etc., todo en asociación con un cliente. En otra implementación, el recurso puede ser una aplicación que se puede utilizar para acceder a información personal e identificable, y utilizar para ayudar al agente al manejar una interacción o cuando está implicado en una interacción con un cliente (e.g., manejar una llamada de servicio al cliente). Dado que el agente está accediendo a los recursos del cliente mientras no maneja una interacción o cuando no participa en una interacción con un cliente (e.g., en una llamada de servicio), se produce una ocurrencia de actividad fraudulenta potencial en la primera vez. Es decir, se deben satisfacer dos criterios para determinar la ocurrencia de una actividad fraudulenta potencial, incluyendo un agente que no está involucrado o no maneja una interacción (e.g., manejando una llamada) con un cliente, y el mismo agente también accede a un recurso con base en el cliente. Como tal, se viola una regla

que indica la ocurrencia de una actividad fraudulenta potencial cuando se cumplen los dos criterios.

1200

[00096] En una implementación, la aplicación es una aplicación no autorizada del cliente. Por ejemplo, el cliente puede estar asociado con dos tipos de aplicaciones: aplicaciones blancas que son accesibles en cualquier momento por el agente, incluso cuando el agente no está involucrado o no maneja una interacción con un cliente (e.g., en una llamada); y las aplicaciones negras enumeradas que sólo son accesibles en una base de necesidad de acceso, tal como cuando el agente está involucrado en o está manejando una interacción (e.g., realizar una llamada de servicio) con un cliente. Por ejemplo, una aplicación en blanco puede incluir una aplicación de entrenamiento que ayuda al agente a tratar diversos tipos de interacciones con un cliente (e.g., tipos y situaciones de hecho de llamadas de servicio). Por otra parte, una aplicación en negro puede incluir una aplicación bancaria que permite a un agente acceder a una o más cuentas bancarias personales asociadas con el cliente y mantenidas por el banco del cliente. En este caso, el acceso a la aplicación bancaria puede estar restringido a veces cuando el agente está manejando una interacción o está involucrado en una interacción con un cliente (e.g., manejando una llamada de servicio) porque no se debe acceder a información personal e identificable cuando la agente no está manejando una interacción y/o no participa en una interacción (e.g., en una llamada) con los clientes.

1220

[00097] En 630, el método incluye recoger pruebas electrónicas de la primera estación de trabajo. Por ejemplo, la evidencia electrónica puede incluir actividades que se realizan sobre los recursos (e.g., sistema de cómputo, teléfono, etc.) de la estación de trabajo, una o más imágenes de la estación de trabajo, una o más imágenes del agente posicionado en la estación de trabajo, imágenes del

1225

escritorio del sistema de cómputo en la estación de trabajo y otras pruebas que identifican al agente posicionado y/o que soportan la verificación de la actividad fraudulenta que se está llevando a cabo en la estación de trabajo.

1230 **[00098]** En una implementación, al recolectar evidencia electrónica, se activa un dispositivo de captura de imagen, y se proporciona una instrucción para capturar al menos una imagen de la estación de trabajo y/o el agente posicionado en la estación de trabajo. Por ejemplo, el dispositivo puede ser parte de un sistema de captura de imágenes que incluye dispositivos instalados estratégicamente (e.g.,
1235 cámaras de alta definición) que se pueden ajustar al zoom para predefinir coordenadas con el propósito de enfocar en una estación de trabajo objetivo y tomar una foto facial de quien atiende en la estación de trabajo objetivo al mismo tiempo que esta ocurriendo la actividad de fraude. Los dispositivos de captura de imágenes pueden estar montados en paredes y/o techos de un piso del centro de
1240 contacto, o un dispositivo integrado dentro de una pantalla de visualización de un recurso de cómputo de una estación de trabajo o un dispositivo situado dentro y dedicado a una estación de trabajo particular.

[00099] En otra implementación, se pueden tomar otras medidas cuando se
1245 determina que se ha producido una actividad fraudulenta potencial con el fin de determinar si ha ocurrido o no fraude real. Estas acciones se pueden tomar automáticamente, o por un especialista de seguridad en un centro de seguridad en tiempo casi real o en un momento posterior. Por ejemplo, una actividad que se realiza por el agente posicionado se puede referenciar con otra actividad que se
1250 realiza por el agente posicionado para determinar si el agente está realizando tareas apropiadas cuando está en la estación de trabajo. Como ilustración, el agente posicionado se puede identificar como un supervisor o cualquier empleado designado a quien se le da una autorización general para acceder a los recursos

del cliente en cualquier estación de trabajo. En otra ilustración, el agente
1255 posicionado puede acceder a las aplicaciones del cliente a las que se puede
acceder en cualquier momento.

[000100] En algunas implementaciones, una vez determinado el fraude real, el
método puede incluir tomar una acción predefinida. Por ejemplo, se puede tomar
1260 una acción adicional para bloquear el acceso fraudulento. Por ejemplo, los
recursos de la estación de trabajo se pueden bloquear y/o asegurar para que no
se puedan tomar acciones con esos recursos. En otra instancia más, una acción
tomada puede incluir el registro de un período predeterminado de actividad del
agente del centro de contacto con fines de evidencia e investigación.

1265
[000101] La FIG. 7A es un diagrama de una tabla 700A que ilustra estaciones de
trabajo y sus ubicaciones dentro de una sección o piso del centro de contacto, en
donde los iconos que representan las estaciones de trabajo se pueden aumentar
para proporcionar información relacionada con el estado de agentes y/o
1270 estaciones de trabajo, así como también información que proporciona la
notificación cuando se detecta actividad fraudulenta potencial en una o más
estaciones de trabajo, de acuerdo con una implementación de la presente
descripción. La generación y mantenimiento del gráfico 700A se puede realizar por
el generador de mapas 265 del centro de seguridad 260 de la FIG. 2, en una
1275 implementación.

[000102] El gráfico 700A ilustra una sección de un centro de contacto. Por
ejemplo, la sección puede ser representativa de un piso de un edificio, o una parte
del piso. Además, el gráfico 700A identifica una pluralidad de estaciones de
1280 trabajo 703, incluyendo la ubicación aproximada de cada estación de trabajo en el
piso. Aunque las formas de implementación de la presente invención describen el

gráfico 700A como proporcionando las ubicaciones de las estaciones de trabajo para incluir el posicionamiento relativo entre las estaciones de trabajo, aunque no necesariamente dibujadas a escala, otras implementaciones proporcionan una
1285 asignación de estaciones de trabajo que puede no ser fiel al posicionamiento real y relativo entre estaciones de trabajo, sino que se utiliza para proporcionar una referencia visual a cada estación de trabajo mostrada en la gráfica 700A. En general, el gráfico 700A proporciona una referencia rápida según las actividades en tiempo real de la pluralidad de agentes en la pluralidad de estaciones de
1290 trabajo 703.

[000103] En la gráfica 700A, cada estación de trabajo está representada por un icono. Por ejemplo, el icono puede ser un rectángulo, que tiene esquinas suaves, como se muestra en la FIG. 7A. Más particularmente, el rectángulo se muestra
1295 como un contorno y/o un límite. Se pueden utilizar variaciones en cómo se presenta el esquema para transmitir información, como el estado de inicio de sesión de un agente que atiende a la estación de trabajo. Por ejemplo, un primer color del contorno indica que un agente está conectado a la estación de trabajo correspondiente. En una implementación, un contorno verde mostrado en el icono
1300 710 de la leyenda 708 y el mapa 700A indica que un agente está conectado a la estación de trabajo. En otro ejemplo, un segundo color del esquema indica que ningún agente está conectado a la estación de trabajo correspondiente. Es decir, la estación de trabajo está inactiva. En una implementación, un contorno gris mostrado en el icono 720 de la leyenda 708 y el mapa 700A indica que un agente
1305 no está conectado. En otro ejemplo, un tercer color del contorno indica que un agente de una estación de trabajo correspondiente está fuera almorzando. En una implementación, un contorno amarillo mostrado en el icono 715 de la leyenda 708 y el mapa 700A indica que un agente de una estación de trabajo correspondiente está almorzando. En otro ejemplo, un cuarto color del contorno indica que la

1310 estación de trabajo correspondiente está bloqueada, por ejemplo, por un agente
que está conectado a esa estación de trabajo. En una implementación, un
contorno rojo mostrado en el icono 725 de la leyenda 708 y el mapa 700A indica
que la estación de trabajo correspondiente está bloqueada. Además, un contorno
en negrita puede indicar que la estación de trabajo correspondiente es
1315 seleccionada por un usuario (e.g., una estación de trabajo actualmente
seleccionada).

[000104] Colocar fondos o rellenos en los iconos que representan estaciones de
trabajo puede proporcionar una referencia rápida a una o más actividades
1320 predefinidas. Por ejemplo, un primer fondo de color del contorno del rectángulo
indica que todo es satisfactorio en la estación de trabajo correspondiente. En una
implementación, un fondo verde mostrado en el icono 730 de la leyenda 708 y el
mapa 700A puede indicar actividad normal en una estación de trabajo
correspondiente, y especialmente que no se ha detectado fraude. En algunas
1325 implementaciones, cuando la actividad del agente viola una regla predefinida, el
fondo del icono correspondiente de la estación de trabajo cambiará a un color
especificado o cambiará de un color (e.g., verde) a otro y proporcionará una alerta
que representa una ocurrencia de evento. En particular, un segundo fondo de
color del contorno rectangular indica que se ha detectado una actividad
1330 fraudulenta potencial en una estación de trabajo correspondiente. En otra
implementación, un fondo amarillo mostrado en el icono 740 de la leyenda 708 y el
mapa 700A indica que la actividad de una estación de trabajo correspondiente
coincide con ciertos criterios que han sido predefinidos como indicando que se ha
producido una actividad fraudulenta potencial. El fondo amarillo proporciona una
1335 notificación visual de la posible actividad fraudulenta que se está llevando a cabo
en una estación de trabajo correspondiente. En otro ejemplo, un tercer fondo de
color del contorno del rectángulo indica que se ha detectado una actividad

fraudulenta potencial y que se debe realizar una revisión de evento adicional para esa estación de trabajo. En una implementación, un fondo rojo mostrado en el
1340 icono 735 de la leyenda 708 y el mapa 700A indica que es necesaria una revisión de evento para la estación de trabajo correspondiente.

[000105] Una vez que el icono cambia a uno de los diversos colores de condiciones no normales, pueden tener lugar acciones adicionales, como la
1345 iniciación de una revisión de evento. Estas acciones se pueden activar automáticamente o puede requerir acciones humanas adicionales que se deben realizar (e.g., revisión de eventos para determinar si se ha producido un fraude real). Por ejemplo, como se describió anteriormente, se registran detalles de la actividad de tal manera que las acciones predefinidas captan la evidencia
1350 necesaria para procesar agentes fraudulentos, así como recopilar la información en tiempo real para fines de investigación. Estos pueden incluir video grabado y/o audio del agente. También pueden incluir la grabación de la actividad de la pantalla del computador y la actividad de grabación en el computador (e.g., acceder a las aplicaciones).

1355
[000106] El contorno y/o el fondo del rectángulo que representa una estación de trabajo se pueden usar conjuntamente con otros iconos, símbolos, sombreados, etc., para proporcionar información relativa a la estación de trabajo correspondiente. Por ejemplo, la información puede representar la actividad de un
1360 agente o el estado emocional de un agente, incluyendo si el agente está manejando una interacción o está involucrado en una interacción con un cliente, en una llamada, en espera, disponible para manejar una interacción, disponible para tomar una llamada, no está disponible para manejar una interacción, no está preparado para tomar otra llamada (e.g., ocupado con una tarea o en otra
1365 llamada), conectado, desconectado, etc. En particular, una señal visual que

representa un estado de actividad se puede colocar en una ubicación en asociación con el icono de la estación de trabajo (e.g., el contorno del rectángulo).

La señal visual puede proporcionar el estado de un agente que atiende a una estación de trabajo correspondiente y/o proporcionar el estado de uno o más

1370 recursos utilizados en una estación de trabajo correspondiente. La ubicación de la señal visual puede estar dentro y centrada en el icono de la estación de trabajo, adyacente a (e.g., lado derecho, lado izquierdo, arriba de y abajo de) el icono de la estación de trabajo, dentro y desplazado a un lado u otro dentro del icono de la estación de trabajo, etc. Las Figs. 7B-K son diagramas de varios símbolos y/o
1375 señales visuales que proporcionan información relacionada con el estado de agentes y/o estaciones de trabajo, así como información que proporciona notificación cuando se detecta actividad fraudulenta potencial en una o más estaciones de trabajo, de acuerdo con una implementación de la presente divulgación.

1380

[000107] La FIG. 7B es una ilustración de un icono 700B que representa una estación de trabajo. El icono 700B también se muestra en la FIG. 7A. El icono 700B puede incluir un símbolo de advertencia 751, en el que un símbolo de advertencia indica generalmente que ha ocurrido un evento que es fuera de lo
1385 normal y puede requerir atención adicional. En una implementación, el símbolo de advertencia está coloreado con un fondo amarillo y un punto de exclamación ennegrecido. Además, la ubicación de un símbolo de advertencia en relación con el contorno 771 del icono 700B puede proporcionar información adicional. Por ejemplo, el símbolo de advertencia 751 que está incluido en el interior del contorno
1390 771, pero desplazado a la derecha del contorno 771, puede indicar que se ha violado un umbral de teléfono. Por ejemplo, es posible que el teléfono esté apagado mientras el agente está conectado a la estación de trabajo, o si el

teléfono no funciona correctamente o si el teléfono se ha puesto en espera durante demasiado tiempo, etc.

1395

[000108] La FIG. 7C es una ilustración de un icono 700C que representa una estación de trabajo. El icono 700C también se muestra en la FIG. 7A. El icono 700C puede incluir un símbolo de advertencia 752, en el que un símbolo de advertencia indica generalmente que ha ocurrido un evento que es fuera de lo normal y puede requerir atención adicional. Además, la ubicación de un símbolo de advertencia en relación con el contorno 772 del icono 700C puede proporcionar información adicional. Por ejemplo, el símbolo de advertencia 752 que está incluido dentro del interior del contorno 772, pero desplazado a la izquierda del contorno 772, puede indicar que se ha infringido un umbral de escritorio. Por ejemplo, el escritorio puede estar apagado mientras el agente está conectado a la estación de trabajo, o el escritorio puede estar funcionando mal, o el escritorio puede haber estado inactivo durante demasiado tiempo, etc.

[000109] En otra implementación, un símbolo de advertencia que está incluido dentro del contorno de un icono, pero está desplazado hacia el centro superior, puede indicar que se ha violado un umbral elevado de la mano. Es decir, puede haber transcurrido demasiado tiempo antes de satisfacer incluso una mano levantada, en la que un acontecimiento elevado de la mano indica que un agente está esperando ser reconocido o está solicitando ayuda del supervisor. Por ejemplo, un símbolo de mano situado en la esquina superior derecha del contorno de un icono puede indicar un evento de mano elevado para la estación de trabajo correspondiente. Además, el símbolo de la mano puede ser de color rosa o rojo para indicar que se requiere atención inmediata. Cuando se ha reconocido y tratado el evento de mano elevado (e.g., un supervisor ha hablado con el agente), entonces el símbolo de mano puede cambiar de color. Por ejemplo, el símbolo de

la mano situado en la esquina superior derecha del contorno del icono puede cambiar de rojo a verde. Después de que se haya tratado el evento de mano elevado, el símbolo de mano se puede retirar del interior del contorno del icono después de un período de tiempo.

1425

[000110] La FIG. 7D es una ilustración de un icono 700D que representa una estación de trabajo. El icono 700D también se muestra en la FIG. 7A. el icono 700D puede incluir un humanoide como torso o busto 754, que generalmente es representativo de un agente. Como se muestra en la FIG. 7D, se muestra un
1430 contorno 773 del busto 754. El contorno 773 puede ser de un primer color e indica que el agente está disponible para manejar una interacción y/o está disponible para participar en una interacción (e.g., tomar una llamada) con un cliente. En una implementación, el contorno 773 está coloreado en verde para indicar que el agente de una estación de trabajo está disponible para manejar una interacción
1435 con un cliente (e.g., listo para tomar una llamada).

[000111] El busto de un agente tal como se representa en un icono se puede colorear o rellenar para proporcionar una referencia rápida a una actividad que está realizando un agente, el estado del agente, el estado emocional del agente o
1440 cualquier otro estado o condición relativa al agente. La FIG. 7E es una ilustración de un icono 700D que representa una estación de trabajo. El icono 700E también se muestra en la FIG. 7A. El icono 700E puede incluir un busto 756, que es generalmente representativo de un agente. Como se muestra, el busto 756 tiene un contorno 774. En este ejemplo particular, un relleno coloreado del busto 756
1445 indica un estado emocional del agente y, en particular, que el agente está satisfecho. Además, el relleno coloreado también puede indicar que el agente está implicado actualmente en una interacción y/o manejar una interacción con un cliente (en una llamada con un cliente) y/o llevar a cabo otras actividades

normales. En una implementación, un relleno verde ilustrado por las líneas diagonales que se inclinan a la izquierda del busto 756 indica que el agente está implicado y/o maneja una interacción con un cliente (e.g., en una llamada), y que todo es normal con el agente y/o la interacción (e.g., llamada). En una implementación, el contorno 774 es del mismo color (e.g., verde).

[000112] La FIG. 7F es una ilustración de un icono 700F que representa una estación de trabajo. El icono 700F también se muestra en la FIG. 7A. El icono 700F puede incluir un símbolo 758 que representa un temporizador de arena (e.g., reloj de arena) e indica que un agente ha puesto a un cliente en espera en una estación de trabajo correspondiente.

[000113] La FIG. 7G es una ilustración de un icono 700G que representa una estación de trabajo. El icono 700G también se muestra en la FIG. 7A. el icono 700G puede incluir un humanoide como el busto 762, que es generalmente representativo de un agente. Como se muestra en la FIG. 7G, se aprecia un contorno 775 del busto 762. El contorno 775 puede ser de un color particular e indica que el agente no está disponible para tomar o involucrarse en y/o no está disponible para manejar una interacción (e.g., una llamada). Por ejemplo, el agente puede estar ocupado completando una tarea (e.g., proyecto, realizando el inicio, etc.). En una implementación, el contorno 775 está coloreado en rojo para indicar que el agente de una estación de trabajo no está disponible para manejar una interacción y/o no está disponible para involucrarse en una interacción (e.g., el agente no está preparado para recibir una llamada).

[000114] La FIG. 7H es una ilustración de un icono 700H que representa una estación de trabajo. El icono 700H se muestra también en la FIG. 7A. El icono 700H puede incluir un busto 764, que es generalmente representativo de un

agente. Como se muestra, el busto 764 tiene un contorno 776 que está coloreado o relleno para proporcionar una referencia rápida a una actividad o estado o condición relativa al agente. En este ejemplo, un relleno de color del busto 764 indica un estado emocional del agente, y en particular que el agente está enojado o agitado. En una implementación, un relleno rojo ilustrado por las rayas cruzadas en el busto 764 indica que el agente está enojado o agitado.

[000115] La FIG. 7I es una ilustración de un icono 700I que representa una estación de trabajo. El icono 700I también se muestra en la FIG. 7A. El icono 700I puede incluir un busto 765 que es generalmente representativo de un agente. Como se muestra, el busto 765 puede estar coloreado o relleno para indicar un estado emocional del agente. Por ejemplo, el relleno puede ser de color rojo, para indicar que el agente está enojado o agitado. Además, el busto 765 puede estar parpadeando, en el que el parpadeo indica que existe un problema subyacente. Por ejemplo, el parpadeo puede indicar que se está produciendo una actividad potencialmente fraudulenta en la estación de trabajo correspondiente. Como ejemplo, es posible que se hayan detectado ciertos criterios durante el monitoreo, tal como que el teléfono está informando que está en una llamada, pero la estación de trabajo informa que está en un estado desconectado o que el teléfono está informando que está en una llamada, pero la estación de trabajo informa que está en un estado bloqueado o de almuerzo.

[000116] La FIG. 7J es una ilustración de un icono 700J que representa una estación de trabajo. El icono 700J se muestra también en la FIG. 7A. El icono 700J puede incluir un busto 768 que es generalmente representativo de un agente. Como se muestra, el busto 768 puede estar coloreado o relleno para indicar un estado emocional del agente. Por ejemplo, el relleno puede estar coloreado de amarillo, para indicar que el agente está estresado.

1505 [000117] Cada uno de los iconos, símbolos, sombreados, etc. utilizados para proporcionar información relativa a una estación de trabajo correspondiente mostrada en las Figs. 7A-J se pueden presentar en cualquier combinación para representar múltiples piezas de información. Por ejemplo, un icono con un fondo de color rojo e incluyendo un busto que tiene un relleno de color verde puede
1510 indicar que el agente está actualmente involucrado en y/o está manejando una interacción con un cliente (e.g., en una llamada) y generalmente se satisface, pero que una ocurrencia de evento (e.g., actividad potencial fraudulenta ha ocurrido) requiere revisión. En otro caso, un busto que tiene un contorno de color verde puede indicar que el agente está disponible para participar y/o manejar una
1515 interacción con un cliente (e.g., tomar una llamada) y tener un relleno que es de color rojo que puede indicar que el agente está enojado o agitado. Esto puede indicar que el agente puede no estar en el mejor estado emocional al manejar la siguiente interacción (e.g., llamada).

1520 [000118] En implementaciones, la revisión de eventos es necesaria para determinar si la actividad fraudulenta potencial que se ha detectado es realmente un fraude. Como se ha comentado anteriormente, la notificación de una revisión de evento se puede presentar a través de un fondo rojo de un icono de estación de trabajo, tal como el icono 735 del gráfico 700A en la FIG. 7A. En una
1525 implementación, el gráfico 700A es visible por un especialista en seguridad (e.g., un "Analista de Riesgo" personal o un especialista/observador de fraude) que supervisa las actividades de los agentes como una responsabilidad a tiempo completo. El especialista en seguridad puede abrir la notificación de revisión de eventos (e.g., fondo rojo en el icono 735) haciendo clic en el icono del cubículo, de
1530 acuerdo con una implementación de la presente descripción. A partir de ahí, el especialista en seguridad puede acceder a información electrónica adicional relacionada con el evento (e.g., la ocurrencia de actividad fraudulenta potencial)

que activó la notificación de la revisión del evento. Por ejemplo, la información puede incluir detalles del evento, fecha y hora de la ocurrencia del evento, nombre
1535 del agente del centro de contacto que está conectado al cubículo, una foto del empleado y una foto de cámara en vivo del agente situado que asiste a la estación de trabajo para fines de comparación y pruebas. Por ejemplo, la información del evento relacionada con un acceso no autorizado de un recurso de cliente puede incluir además del anterior, el estado de un agente con respecto a la manipulación
1540 o participación en una interacción, el estado de llamada del agente (e.g., no listo y/o no contesta la llamada), el desde la última entrada en el recurso de computo (e.g., 0,41 segundos), tiempo transcurrido desde el manejo de la última interacción (e.g., segundos desde la última llamada), una dirección de protocolo de Internet (IP) de un recurso de cliente accedido, la marca de tiempo de la alerta y un
1545 mensaje que proporciona información adicional.

[000119] En una implementación, el especialista en seguridad tiene la capacidad de conectarse remotamente a la estación de trabajo en tiempo real, permitiendo así que el especialista de seguridad vea exactamente lo que el agente posicionado
1550 ve en su pantalla. Además, las pruebas se capturan electrónicamente durante este período. Esto permite al especialista de seguridad observar las actividades del agente posicionado, tal como observar los accesos a los recursos del cliente. Por ejemplo, una actividad tal como la visualización de una o varias informaciones personales e identificables del cliente sin estar involucrada en interacciones con
1555 dichos clientes (e.g., no gestionar una llamada con esos clientes) es una indicación significativa de actividad fraudulenta. En algunas implementaciones, la revisión de eventos se maneja automáticamente, por ejemplo utilizando reglas que definen comportamiento o actividad fraudulenta y determinando si la evidencia de actividad fraudulenta potencial coincide con dichas reglas. En otras
1560 implementaciones, la revisión de la actividad del agente y/o evidencia en relación

con una notificación del evento de actividad fraudulenta potencial se produce en un momento posterior. Es decir, la actividad del agente, así como cualquier desencadenador (e.g., notificación de evento, violaciones de reglas, etc.) de la actividad fraudulenta potencial se almacena y se accede en un momento posterior para el análisis.

[000120] Una vez que una actividad ha sido clasificada como fraudulenta, se pueden tomar medidas adicionales en un esfuerzo por frenar futuros casos de fraude por parte del agente que comete el fraude y por otros agentes del centro de contacto que son conscientes del fraude cometido. Es decir, la aplicación de las consecuencias negativas contra un agente que ha demostrado estar cometiendo fraude actuará para disuadir la futura actividad fraudulenta de otros agentes del centro de contacto que son conscientes de las consecuencias negativas. El conocimiento por los agentes de que el centro de contacto tiene controles para luchar contra el fraude puede proporcionar un disuasivo necesario y suficiente para la ejecución de futuras actividades fraudulentas. Las consecuencias negativas para un agente que comete una actividad fraudulenta pueden incluir la confrontación pública del agente, la pérdida de empleo y la posible persecución civil y/o penal. Para ilustrar, una vez que se ha verificado la actividad fraudulenta, un representante del centro de contacto (e.g., recursos humanos, gerente de cuenta, supervisor, especialista en seguridad, etc.) puede confrontar públicamente al agente en su estación de trabajo y/o en el piso del centro de contacto. El agente es escoltado fuera de la estación de trabajo y alejado del piso del centro de contacto. El agente es terminado, y escoltado adicional fuera del centro de contacto. Se puede contactar a la policía pública para abrir un caso. El agente puede además ser procesado en cortes civiles y/o criminales usando la evidencia recopilada por las implementaciones de la presente invención, como se describió anteriormente.

[000121] Pueden adoptarse medidas adicionales para reducir y prevenir la
1590 aparición de actividad fraudulenta. Por ejemplo, se puede llevar a cabo una sólida
formación de concientización sobre la seguridad, como durante la iniciación del
empleo y, además, periódicamente. Se debe firmar un acuerdo de no divulgación
para verificar que el agente es consciente de los problemas de seguridad.
Además, se pueden realizar verificaciones de antecedentes sobre posibles
1595 empleados, por ejemplo, para filtrar a personas que se sabe que han cometido
fraude. En otro ejemplo, se envían mensajes electrónicos que indican qué
actividades se autorizan para un agente en particular en un momento
determinado. Por ejemplo, una vez que un agente termina una interacción con un
cliente (e.g., termina con una llamada), uno o más mensajes se pueden entregar
1600 para su visualización en una pantalla visible por el agente, en la que los mensajes
enumeran ambas acciones autorizadas que (e.g., acceder a los recursos de
capacitación, las aplicaciones de la lista blanca, etc.) y las acciones no autorizadas
que el agente no debe realizar (e.g., acceder a las aplicaciones de la lista negra,
acceder a los recursos del cliente con información personal e identificable, etc.).
1605 En otro ejemplo, un entorno de "escritorio limpio" se aplica en las estaciones de
trabajo del centro de contacto. Es decir, los agentes no pueden traer artículos
personales al centro de contacto, aparte de la ropa que usan. Los artículos
personales (e.g., papel, lápiz, etc.) que pudieran utilizarse para "extraer"
información del centro de contacto están estrictamente prohibidos en el centro de
1610 contacto. Otras medidas utilizadas para prevenir el fraude son implementables y
usadas en combinación con implementaciones de la presente invención.

[000122] Por lo tanto, de acuerdo con implementaciones de la presente
invención, se describen métodos y sistemas para detectar y prevenir el fraude
1615 dentro de un centro de contacto.

[000123] Aunque la descripción anterior presenta varias implementaciones usando diagramas de bloques específicos, diagramas de flujo y ejemplos, cada componente de diagrama de bloques, etapa de diagrama de flujo, operación y/o
1620 componente descrito y/o ilustrado en el presente documento se pueden implementar individualmente y/o colectivamente. Además, cualquier descripción de componentes contenidos dentro de otros componentes se debe considerar como ejemplos porque muchas otras arquitecturas se pueden implementar usando los principios inventivos descritos en el presente documento.

1625

[000124] Los parámetros del proceso y la secuencia de etapas descritos y/o ilustrados en el presente documento se dan a modo de ejemplo solamente y se pueden variar según se desee. Por ejemplo, aunque las etapas ilustradas y/o descritas aquí se pueden mostrar o discutir en un orden particular, estas etapas no
1630 necesariamente se deben realizar en el orden ilustrado o discutido. Los diversos métodos de ejemplo descritos y/o ilustrados aquí también pueden omitir una o más de las etapas descritas o ilustradas en el presente documento o incluir etapas adicionales además de las descritas.

1635

[000125] Aunque se han descrito y/o ilustrado diversas implementaciones en el contexto de sistemas de computación completamente funcionales, una o más de estas formas de implementación de ejemplo se pueden distribuir como un producto de programa en una variedad de formas, independientemente del tipo particular de computador - medios de lectura que se utilizan para realizar
1640 realmente la distribución. Las implementaciones aquí descritas también se pueden implementar utilizando módulos de software que realizan ciertas tareas. Estos módulos de software pueden incluir secuencias de comandos, lotes u otros archivos ejecutables que se pueden almacenar en un medio de almacenamiento legible por computador o en un sistema de cómputo. Estos módulos de software

1645 pueden configurar un sistema de cómputo para llevar a cabo una o más de las implementaciones de ejemplo descritas en el presente documento. Uno o más de los módulos de software descritos en el presente documento se pueden implementar en un entorno de computación en nube. Los entornos de computación en nube pueden proporcionar varios servicios y aplicaciones a través
1650 de Internet. Estos servicios basados en la nube (e.g., software como servicio, plataforma como servicio, infraestructura como servicio, etc.) pueden ser accesibles a través de un navegador Web u otra interfaz remota. Se pueden proporcionar varias funciones descritas en el presente documento a través de un entorno de escritorio remoto o cualquier otro entorno informático con base en la
1655 nube.

[000126] La descripción anterior, con fines de explicación, se ha hecho con referencia a implementaciones específicas. Sin embargo, las discusiones ilustrativas anteriores no pretenden ser exhaustivas o limitar la invención a las
1660 formas precisas descritas. Son posibles muchas modificaciones y variaciones en vista de las enseñanzas anteriores. Las implementaciones se eligieron y describieron con el fin de explicar mejor los principios de la invención y sus aplicaciones prácticas, para permitir así a los versados en el arte utilizar mejor la invención y diversas implementaciones con diversas modificaciones que pueden
1665 ser adecuadas para el uso particular contemplado.

[000127] Se describen así implementaciones de acuerdo con la invención. Aunque la presente descripción ha sido hecha en implementaciones particulares, se debe apreciar que la invención no debe ser interpretada como limitada por tales
1670 implementaciones.