Industria y Comercio
SUPERINTENDENCIA

...ado para el adhesivo de radicación
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
No. 14-148865- -00002-0000
Fecha: 2014-10-16 16:47:41 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
Act. 400 OPOSIOBSERVTER Folios: 38

DIRECCIÓN DE NUEVAS CREACIONES
PRESENTACIÓN DE OPOSICIÓN

1. Oposición a solicitud de:

X Patente de invención
☐ Registro de Diseño Industrial
☐ Patente de Modelo de Utilidad
☐ Esquema de Trazado de Circuitos Integrados

Número de expediente: **14-148865**

Solicitante: **SMART HUB PTE. LTD**

Apoderado: **SILVANA MARÍA LÓPEZ DÍAZ**

Título de la Nueva Creación: **SISTEMA, MÉTODO Y PROGRAMA COMPUTACIONAL ADAPTADO PARA FACILITAR UNA TRANSACCIÓN.**

Gaceta: **700 del 21 de Julio de 2014**

2. Datos del Opositor

X Persona Natural ☐ Persona Jurídica

DAVID LEONARDO HURTADO
Nombre o denominación /Razón social completa

Nombre del representante legal

Documento de identificación: C.C. **X** C.E ☐ NIT ☐ Otro ☐ Cuál _

Número 94.552.179

Dirección Cra 79 # 13B -159 Ciudad Bogotá

Teléfono 7496888 **Fax:** 2481211 **Correo electrónico** notificaciones@munozab.com

3. Datos del representante o apoderado:

LOLA KANDELAFT	423.178	233.326 del C.S. de la J.
Apellidos y Nombre	**Documento de identificación**	**Tarjeta profesional**

Dirección del representante		
Carrera 5ta # 66-17		
Dirección electrónica	No. Fax	Número telefónico
notificaciones@munozab.com	2481211	7496888

En caso de haber presentado poder general para asuntos que se adelanten ante la Delegatura de Propiedad Industrial, sírvase indicar el número de su radicación o protocolo de poder general:

4. Fundamentos de la oposición

Causal:

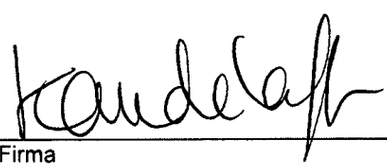
Son fundamentos de derecho los artículos 14 a 20 De Los Requisitos de Patentabilidad, el artículo 30 De las Solicitudes de Patente y los artículos 42 y 43 Del trámite de la solicitud (Oposiciones), de la Decisión 486 de 2000.

Justificación
Referirse al Escrito de Oposición

Prórroga: **SI** ☐ **NO** **X**

5. Anexos

- **X** Comprobante de pago de la tasa.
- **X** Poder, si fuera el caso.
- **X** Fundamentos de la oposición. Se anexan ___ folios (obligatorios indicar cuántos).
- **X** Anexo de fundamentos de la oposición. Se anexan ____folios (obligatorios indicar cuántos)
- ☐ Copias para traslado.
- ☐ Copia de la solicitud y sus anexos en formato magnético.

6. Firma	
LOLA KANDELAFT	
Nombre del Firmante	Firma
423.178	233.326 del C.S. de la J.
C.E	Tarjeta Profesional

muñoz°abogados

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

Señores
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
E. S. D.

Expediente:	**14-148865**
Título Solicitado:	**SISTEMA, MÉTODO Y PROGRAMA COMPUTACIONAL ADAPTADO PARA FACILITAR UNA TRANSACCIÓN.**
Publicación:	**Gaceta 700 del 21/07/2014, número de publicación 748.**
Solicitante:	**SMART HUB PTE. LTD**
Opositor:	**DAVID LEONARDO HURTADO**
Trámite:	**PRESENTACIÓN DE OPOSICION**

LOLA KANDELAFT, *mayor de edad, identificada como aparece al pie de mi firma,* obrando en calidad de apoderada de **DAVID LEONARDO HURTADO**, en ejercicio de lo dispuesto por el artículo 42 de la Decisión 486 de 2000, muy respetuosamente me permito presentar oposición en contra de la solicitud de patente "SISTEMA, MÉTODO Y PROGRAMA COMPUTACIONAL ADAPTADO PARA FACILITAR UNA TRANSACCIÓN" *presentada a nombre de la sociedad* **SMART HUB PTE. LTD**, *de acuerdo con las* siguientes consideraciones:

I. LEGÍTIMO INTERÉS

El interés manifestado por mi poderdante **DAVID LEONARDO HURTADO** para presentar esta oposición, se establece a partir de que, como persona natural y consumidor de los servicios prestados por entidades financieras, al ser acreedor de tarjetas debido y crédito, además de hacer uso de diferentes canales de transacción asociados a actividades económicas, considera que otorgar protección a una patente *como la solicitada vulneraría sus derechos, en tanto que la concesión de esta incurriría* en una afectación directa al sector bancario como a los consumidores, toda vez que los demás actores se verían obligados a cambiar la calidad de sus servicios al margen de evitar la infracción del derecho que se conferiría al solicitante.

II. ANTECEDENTES

3.1. Mediante escrito radicado ante la Superintendencia de Industria y Comercio el día 10 de Julio de 2014, SMART HUB PTE. LTD., entró a fase nacional en Colombia con la solicitud de patente de invención titulada "SISTEMA, MÉTODO Y PROGRAMA COMPUTACIONAL ADAPTADO PARA FACILITAR UNA TRANSACCIÓN", *la cual corresponde* a la solicitud internacional PCT/SG2013/000006 del 04 de Enero de 2013; publicada internacionalmente con el número WO20130103323 el 11 de Julio de 2013.

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

3.2. La solicitud fue publicada mediante número de publicación 748, en la Gaceta 700 de la Propiedad Industrial del 21 de Julio de 2014.

3.3. En uso de las facultades legales conferidas y estando dentro de la oportunidad legal, esta parte se permite presentar escrito de oposición en contra de la solicitud inicialmente elevada a su Despacho.

III. FUNDAMENTO DE LA OPOSICIÓN

Antes de entrar a esbozar a profundidad los argumentos jurídicos que ameritan la negación del registro que se tramita a través del presente expediente, vemos totalmente prudente y necesario considerar el efecto negativo que tendría la concesión de dicha patente para el consumidor en general.

En efecto, la sociedad **SMART HUB PTE. LTD.,** mediante la presente solicitud de registro, está tratando de obtener derechos exclusivos de propiedad industrial, a saber los derechos otorgados por una patente de invención, cuando la supuesta invención no es más que un programa de ordenador o software.

En tal virtud, en la Comunidad Andina, el software se encuentra protegido, de conformidad con lo establecido en la Ley 23 de 1982 y el Decreto 1360 de 1989, mediante el **Registro Nacional de Derecho de Autor** y no mediante la modalidad patente de invención y/o modelo de utilidad. Por lo tanto, la protección de la obra referida en la presente solicitud debe tramitarse ante la Dirección Nacional de Derechos de Autor, y no ante la Superintendencia de Industria y Comercio.

Si no fuera suficiente, la supuesta invención, de ser considerada como tal, no cumple con los criterios de novedad y nivel inventivo necesarios a la obtención de una patente.

Así las cosas, la solicitud de la referencia no representa un material patentable en conformidad con la normatividad Andina desde diferentes perspectivas legales que se presentarán a continuación:

3.1. Exclusiones de Patentabilidad

De acuerdo a lo descrito por la Decisión 486 de 2000 de la Comunidad Andina de Naciones, que en su artículo 15 establece los objetos que no se consideran invenciones, entre los que se encuentran *"e) los programas de ordenadores o el soporte lógico, como tales; y, f) las formas de presentar información"*. Así las cosas, los *software*, como el descrito en la tecnología presentada por el solicitante, se encuentran excluidos del derecho de patente.

Por lo tanto, es preciso recordar lo que el Tribunal de Justicia de la Comunidad Andina establece por "invención" con el fin de demostrar que el programa de ordenador, o mal llamado "dispositivos informático", no pertenece a ninguna de las definiciones expuestas.

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email info@munozab.com
Bogotá, Colombia

"En el ámbito de la doctrina la invención ha sido considerada como la solución de un problema técnico aplicable a la industria, y que proporciona la posibilidad de obtener un cierto resultado útil (BAYLOS CORROZA, Hermenegildo: Tratado de Derecho Industrial, segunda edición, Editorial Civitas, 1993, p. 695).

"También ha sido definida la invención como una regla para el obrar humano que contiene la solución a un problema técnico hasta entonces no resuelto o resuelto de manera insatisfactoria (OTERO LASTRES, José Manuel: Seminario sobre patentes en la Comunidad Andina: "La invención y las excepciones a la patentabilidad en la Decisión 486 del Acuerdo de Cartagena". Quito, 9 de mayo de 2001, CORPIC).

"La invención puede recaer sobre una entidad física (producto, dispositivo, máquina, sustancia, composición) o sobre una actividad (procedimiento, método, utilización).

En el caso de la invención de producto, el objeto inventivo se halla constituido por un cuerpo cierto destinado a llenar una necesidad industrial que el estado de la técnica no ha podido satisfacer. En cambio, en el caso de la invención de procedimiento, el objeto inventivo se halla constituido por "una serie o sucesión de operaciones que inciden sobre una materia (sólida, líquida o gaseosa) que se encamina a la obtención de una cosa o de un resultado" (OTERO LASTRES, José Manuel: op. cit).

"Por su parte, el Tribunal ha dicho que "el concepto de invención, a efectos de ser objeto de una concesión de patentes, comprende todos aquellos nuevos productos o procedimientos que, como consecuencia de la actividad creativa del hombre, impliquen un avance tecnológico —y por tanto no se deriven de manera evidente del 'estado de la técnica'—, y además sean susceptibles de ser producidos o utilizados en cualquier tipo de industria" (Sentencia dictada en el Proceso N° 21-IP-2000, del 21 de octubre de 2000, publicada en la G.O.A.C. A/° 631, del 10 de enero de 2001, caso "DERIVADOS DE BILIS HUMANA)". [1]

En el caso que nos interesa, es claro que la tecnología descrita y reivindicada en la solicitud de patente de la referencia no responde a los criterios arriba establecidos, por no *consistir* en una serie o sucesión de operaciones que inciden sobre una materia (sólida, líquida o gaseosa) que se encamina a la obtención de una cosa o de un resultado.

Por otro lado, según lo establecido en el artículo 23 de la Decisión 351 del Acuerdo de Cartagena, "***Los programas de ordenador se protegen en los mismos términos que las obras literarias***. *Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto*".

[1] TJCA, Proceso No. 43-IP-2002,

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

En donde la misma decisión en el Artículo 3 define los programas de ordenador (software) de la siguiente manera:

> *"Expresión de un conjunto de **instrucciones** mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador -un aparato electrónico o similar capaz de elaborar informaciones-, **ejecute determinada tarea u obtenga determinado resultado**. El programa de ordenador comprende también la documentación técnica y los manuales de uso."*
>
> (Negrilla fuera de texto)

Por todo lo anterior, la materia presentada como invención en la solicitud de la referencia no cumple con los criterios de patentabilidad dispuestos en la Legislación andina en materia de patentes, en tanto que no corresponde con una invención. Adicionalmente se recuerda que el hecho de presentar la tecnología como un "dispositivo informático" en contra de la esencia de la misma no es suficiente para que la tecnología sea considerada como una invención, y por ende ser materia patentable.

3.2. Falta de Claridad

Adicionalmente, la GUÍA PARA EXAMEN DE SOLICITUDES DE PATENTE DE INVENCIÓN Y MODELO DE UTILIDAD de la Superintendencia de Industria y Comercio, en la cual se instauran las características que debe tener una reivindicación de producto en caso de que este realmente lo fuera, se establece lo siguiente:

> *"El examinador debe tener en cuenta que las reivindicaciones son cláusulas que delimitan el objeto para el que se solicita la protección. Mencionan las características técnicas esenciales del objeto reivindicado"* Página 68.
>
> *"Las reivindicaciones deben contener todas las características técnicas esenciales de la invención las cuales definen la invención y la hacen (o deberían hacerla) diferente del estado de la técnica y, por tanto, constituyen la solución al problema técnico que intenta resolver la invención.*
>
> *Para efectos del examen, los términos relativos a aspectos no técnicos, tales como **resultados alcanzados, por ejemplo las ventajas comerciales, no se consideran como características técnicas de la invención**, dado que no son características esenciales y restan claridad a la reivindicación. Por lo tanto, el examinador debe hacer el requerimiento al solicitante para que retire los resultados a alcanzar tanto del preámbulo como de la parte característica de las reivindicaciones."* Página 69
>
> (Énfasis fuera del texto)

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

Por lo que las reivindicaciones, tal y como las presenta el solicitante no cumplen con las características establecidas en dicha guía para cumplir con el requisito de claridad establecido en el artículo 30 de la Decisión 486 que cita "Las reivindicaciones definirán la materia que se desea proteger mediante la patente. **Deben ser claras y concisas** y estar enteramente sustentadas por la descripción".

Por el contrario presenta materia muy general que no permite diferenciar a la tecnología del estado de la técnica y por lo tanto su protección sería perjudicial para el sector financiero al incluir cualquier desarrollo informático o financiero con características similares.

3.3. Falta de Novedad y Nivel Inventivo

Dentro de la documentación presentada por la firma solicitante, presentan de manera conveniente el Reporte Preliminar Internacional de Patentabilidad correspondiente al Capítulo II del reporte, emitido por la oficina Australiana de patentes, el cual presenta un concepto favorable para la solicitud a partir de las modificaciones realizadas.

No obstante, el solicitante omite el Capítulo I del mismo reporte el cual presenta un concepto desfavorable, asegurando que la patente carece de novedad en sus reivindicaciones 1, 3, 5-8 y 12 a 17, en consideración del Documento presentado a continuación, y con las siguientes objeciones relativas a la novedad y el nivel inventivo de la solicitud:

Item	Documento	Título	Fecha de Publicación
D1	US7383988	"System and method for locking and unlocking a financial account card"	10 de Junio de 2008

Reivindicaciones 1, 8 y 15 a 17: el documento divulga un sistema y método mediante el cual el titular de una cuenta de tarjeta financiera como una tarjeta de crédito o una tarjeta debido puede deshabilitar o rehabilitar el uso de la tarjeta bloqueando y desbloqueando la tarjeta repetidamente. La solicitud de desbloqueo o bloqueo de una tarjeta puede realizarse por una variedad de canales de envío como teléfonos, cajeros automáticos, en línea, entre otros. Para una transacción de bloqueo, el procesador de tarjeta guarda el estado operable actual de la tarjeta y cambia el estado a bloqueado. Para una transacción de desbloqueo, el estado operable guardado de la tarjeta es reestablecido. El estado cambiado de la tarjeta de bloqueado a o desbloqueado es reportado por el procesador de tarjeta a los sistemas e acompañamiento y un registro de auditoría creado. Varios indicadores o códigos de estado son asociados con cada número de tarjeta y mantenidos en una base de datos de tarjetas. El estado operable actual de la tarjeta es determinado por la condición de estos varios indicadores o códigos. Una respuesta es enviada de vuelta del procesador de tarjeta vía el canal de envío al canal del dueño indicando que la solicitud de bloqueo o desbloqueo de la operación de

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

la tarjeta ha sido recibida y realizada, como se puede ver en el sumario de la invención, Columna 8 líneas 60-66.

Reivindicaciones 3, 5 y 10 a 12: el documento D1 divulga un "host intermediario supiente en forma de un "sistema de acompañamiento". Un sistema de acompañamiento en frente del procesador de tarjeta puede sustituir el procesador de tarjeta y tomar la decisión de autorización sin pasar la solicitud de procesador de tarjeta, ver columna 9 líneas 21-53,

Reivindicaciones 6 y 13: el documento D1 divulga que los Indicadores o códigos de estado en las bases de datos son actualizados en todo momento si la tarjeta es bloqueada o desbloqueada por el titular de la tarjeta, ver Columna 9, líneas 4-8,

Reivindicaciones 7 a 14: el documento D1 divulga un sistema y método a partir del cual un titular de una cuenta de tarjeta financiera como una tarjeta de crédito o una tarjeta debido puede deshabilitar o rehabilitar el uso de la tarjeta bloqueando y desbloqueando la tarjeta repetidamente, Ver sumario de la Invención

Con respecto al nivel inventivo, se considera que las reivindicaciones citadas anteriormente que carecen de novedad, y bajo el mismo concepto carecen de nivel inventivo, no obstante las reivindicaciones restantes, **reivindicaciones 2, 4, 9 y 11**, se consideran características adicionadas a la invención relativas a arreglos que corresponden netamente a material opcional de diseño, en donde es usado el conocimiento general de la técnica sobre el estado del arte, por lo que no pueden contribuir a conferir nivel inventivo a la "Invención"; por lo cual las reivindicaciones 1 a 17 carecen de Nivel Inventivo.

En respuesta al concepto formulado por la Oficina Australiana de Patentes, el solicitante realizó cambios al capítulo reivindicatorio limitados a cambiar la expresión "*al menos un canal de transacción relativamente inseguro de UNO O MAS canales de transacción*" por la expresión "*al menos un canal de transacción relativamente inseguro de UNA PLURALIDAD DE canales de transacción*".

A partir de dichos cambios, el solicitante argumenta que dicha salvedad confiere novedad a la "invención", en tanto que la diferencia fundamental de la "invención" con el antecedente citado radica en que el sistema de bloqueo y desbloqueo del documento D1 se dirige al bloqueo de la tarjeta en su totalidad, es decir, que todos los posibles canales de transacción se ven afectados por dichos bloqueos. Por otro lado, su tecnología se fundamenta en el bloqueo o desbloqueo de canales de transacción específicos de naturaleza relativamente insegura, lo que la hace superior a la tecnología descrita en el documento D1, permitiendo una flexibilidad al usuario para utilizar varios canales de transacción y configurar su estado de bloqueo/desbloqueo convenientemente.

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email info@munozab.com
Bogotá, Colombia

A partir de lo anterior, es necesario establecer los argumentos del solicitante no son válidos, de acuerdo con lo siguiente:

En la columna 4, líneas 6-10, el Documento D1 divulga "*el titular de la tarjeta 12 puede también recibir una solicitud de indicar si el titular 12 le gustaría bloquear 16 o desbloquear 18 la tarjeta, o realizar alguna otra transacción, como acceder a una cuenta subyacente, hacer un retiro, etc...*" lo que demuestra que la posibilidad de bloquear o desbloquear transacciones específicas ya fue considerada en este documento, por lo que esta característica de ninguna manera confiere novedad a la "invención" del solicitante.

Adicionalmente, el bloqueo independiente de diferentes canales de transacción, no solo se encuentra contemplado el documento D1, pero la opción de bloquear específicamente canales de transacción hace parte del estado de la técnica, pues obedece a una práctica comúnmente realizada por los bancos, dada su consciencia de la relativa inseguridad de algunos de estos, como se puede ver en los documentos citados a continuación.

Ítem	Documento	Título	Fecha de Publicación
D2	Norma 052	Capítulo décimo segundo: requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios.	Octubre de 2007
D3	Anexo Contrato de Servicios	Anexo al contrato de servicios electrónicos. Autorización para realizar transacciones en canales electrónicos.	23 de Marzo de 2009
D4	US2010312700	System and method for managing status of a payment instrument.	09 de Diciembre de 2010

Los documentos D2 y D3 representan documentos de entidades financieras que evidencian que la práctica de bloquear canales de transacciones es prevista no solo como requerimientos mínimos dictados por la Superintendencia Financiera de Colombia para garantizar la seguridad de los servicios prestado, como se evidencia en el documento D2, sino también como parte de los servicios electrónicos prestados por las entidades financieras como en Banco Internacional, como se evidencia en el documento D3.

El documento D2, en el capítulo 3 de las obligaciones generales de las entidades sometidas a la inspección y vigilancia de la Superintendencia de Industria y Comercio, establece en su numeral 3.1.12. "Establecer procedimientos para el bloqueo de canales o de medios, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos." , en donde la expresión *canales* fue definida en el capítulo anterior como "a) Oficinas. b) Cajeros Automáticos (ATM). c) Receptores de cheques. d) Receptores de dinero en efectivo. e) POS (incluye PIN Pad). f) Sistemas de Audio Respuesta (IVR). g) Centro de atención telefónica (Call Center, Contact Center). h) Sistemas de acceso remoto para clientes (RAS). I) Internet.

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

j) Dispositivos móviles." de manera compatible con la definición propuesta por el solicitante.

El documento D3, presenta un formulario, en el cual el cliente, titular de un servicio electrónico, tiene la facultad de señalar las transacciones que desea bloquear de la siguiente manera:

BLOQUEO DE TRANSACCIONES EN CANALES ELECTRONICOS * Marcar con una X la transacción que desea bloquear				
TRANSACCION	BANCA EN LINEA	TERMINAL DE CONSULTA	INTERCENTER	CAJERO AUTOMATICO
Consulta de productos generales				
Compras				
Pagos				
Solicitudes				
Transferencias				
Otro:				

Por su parte, el documento D4 presenta un servicio de procesamiento de transacciones que permite a un cliente para cambiar selectivamente el estado de una cuenta de **asociado con un instrumento de pago** mediante la activación o desactivación de la cuenta. El servicio Intermediario puede administrar el estado de cuenta de forma local mediante un módulo de reglas. Como alternativa, la entidad emisora puede administrar el estado de cuenta, mientras que el servicio de intermediación proporciona una Interfaz para los clientes. Un cliente se comunica con el servicio de intermediación para dirigir el servicio para cambiar el estado de la cuenta. El servicio de Intermediación determina la institución emisora de la cuenta y proporciona una Indicación de la entidad emisora de la situación actual de la cuenta (o del cambio en el estado). El servicio de mediación puede proporcionar la información, mediante la transmisión de un mensaje a la entidad emisora o mediante el almacenamiento de la información del estado de cuenta en su propia base de datos. La entidad emisora podrá entonces solicitar el estado de cuenta del servicio de intermediación cada vez que necesita la información, como cuando se recibe una solicitud de autorización.

De acuerdo a lo anterior, la "invención" solicitada bajo el expediente impugnado no cumple con los requisitos de novedad y nivel inventivo, y los argumentos y modificaciones presentados por el solicitante en el Capítulo II del Reporte Preliminar Internacional de Patentabilidad no son suficientes para cambiar dicha condición.

En este sentido, es posible establecer que la solicitud de referencia no cumple con las disposiciones legales establecidas para la obtención de una patente de invención, desde la exclusión de patentabilidad por no corresponder a una invención, hasta la falta de Novedad, Nivel Inventivo y Claridad, que la hacen incompatible con el sistema de patentes de la Comunidad Andina de Naciones.

www.munazab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munazab.com
Bogotá, Colombia

IV. PETICIONES

Que se niegue el beneficio de Patente de Invención a la solicitud titulada SISTEMA, MÉTODO Y PROGRAMA COMPUTACIONAL ADAPTADO PARA FACILITAR UNA TRANSACCIÓN, contenida en el expediente **14 148.865** solicitado por la Sociedad SMART HUB PTE. LTD por no cumplir con los requisitos de patentabilidad dispuestos en la Decisión 486 de 2000, con base en los fundamentos expuestos anteriormente por esta parte en contra de la solicitud presentada por **SMARTH HUB PTE. LTD.** y en el mismo sentido se declare fundada la presente Oposición.

V. FUNDAMENTOS DE DERECHO

Son fundamentos de derecho los artículos 14 a 20 De Los Requisitos de Patentabilidad, el artículo 30 De las Solicitudes de Patente y los artículos 42 y 43 Del trámite de la solicitud (Oposiciones), de la Decisión 486 de 2000.

VI. PRUEBAS

Ruego que se tengan como tales, sin perjuicio de las que puedan presentarse al vencimiento de la prórroga solicitada, y de aquellas que el Despacho considere oficiosamente, las siguientes:

6.1. copia del Reporte de Búsqueda Internacional PCT. Capítulo I.
6.2. Copia del Documento D1 el cual se encuentra en las bases de datos de acceso público para su consulta.
6.3. Copia del Documento D2 tal y como se encuentra disponible en línea para su consulta.
6.4. Copia del Documento D3 tal y como se encuentra disponible en línea para su consulta.
6.5. Copia de la información bibliográfica y las reivindicaciones del Documento D4 el cual se encuentra en las bases de datos de acceso público para su consulta.

VII. ANEXOS

Para efectos del trámite correspondiente, me permito anexar al presente escrito los siguientes anexos

7.1. Poder para actuar.
7.2. Constancia de pago de las tasas de tramitación de oposición.
7.3. El mencionado en el acápite de pruebas.

www.munozab.com
Carrera 5 No 66 – 17
Tel. (57 1) 749 68 88
Fax. (57 1) 481 83 04
Email. info@munozab.com
Bogotá, Colombia

VIII. NOTIFICACIONES

La Solicitante y el suscrito, recibiremos notificaciones en la Secretaría de su Despacho y en la Carrera 5 # 66-17 de Bogotá D. C.

Cordialmente,

LOLA KANDELAFT
C.E. 423.178
T.P. 233.326 del C.S. de la J.

Industria y Comercio
SUPERINTENDENCIA

DELEGATURA PARA LA PROPIEDAD INDUSTRIAL
FORMULARIO PARA OTORGAR PODER A ABOGADO
EN LOS TRÁMITES DE PROPIEDAD INDUSTRIAL

1. Datos del otorgante:

X Persona Natural ☐ Persona Jurídica

Nombre: DAVID LEONARDO HURTADO

Tipo de empresa: ☐ Micro ☐ Pequeña ☐ Mediana ☐ Otra:

Documento de identificación: X C.C. ☐C.E. ☐NIT ☐Otro Número: 94.552.179

Nacionalidad / País de constitución	Dirección y Domicilio del otorgante	
Colombia	Cra 79 # 13B -159	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	2481211	7496888

2. Datos del apoderado:

Guillermo Andrés Navarro Romero — Apellidos y Nombre
80.111.198 de Bogotá — Documento de identificación
208.987 del C. S. de la J. — Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	Carrera 5 No. 66-17	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	2481211	7496888

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.1. Datos del apoderado:

Diego Muñoz Marroquín — Apellidos y Nombre
7.688.292 de Neiva — Documento de identificación
134.000 del C. S. de la J. — Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	Carrera 5 No. 66-17	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	2481211	7496888

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.3. Datos del apoderado:

Arleth Aroca Almanza	36.718.415 de Santa Marta	123.758 del C. S. de la J.
Apellidos y Nombre	Documento de identificación	Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	**Carrera 5 No. 66-17**	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	**2481211**	**7496888**

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.4. Datos del apoderado:

Catherine Zea Velásquez	53.164.779 de Bogotá	162.381 del C. S. de la J.
Apellidos y Nombre	Documento de identificación	Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	**Carrera 5 No. 66-17**	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	**2481211**	**7496888**

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.5. Datos del apoderado:

Liliana Hoyos Celis	52.388.158 de Bogotá	211.266 del C. S. de la J.
Apellidos y Nombre	Documento de identificación	Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	**Carrera 5 No. 66-17**	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	**2481211**	**7496888**

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.6. Datos del apoderado:

Nicolás Polanía Tello	12.265.099 de Pitalito	154.131 del C. S. de la J.
Apellidos y Nombre	Documento de identificación	Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	**Carrera 5 No. 66-17**	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	**2481211**	**7496888**

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

2.7. Datos del apoderado:

Lola Pol Elvire Kandelaft	C.E. 423178	233326 del C. S. de la J.
Apellidos y Nombre	Documento de identificación	Tarjeta Profesional

Nacionalidad / País de constitución	Dirección del apoderado	
Colombiana	**Carrera 5 No. 66-17**	
Dirección Electrónica	No. Fax	Número Telefónico
notificaciones@munozab.com	**2481211**	**7496888**

X Autorizo expresamente a la Superintendencia de Industria y comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico.

14

3. Actuaciones en cuestión:

Este poder concierne:

X Todas las solicitudes y/o registros actuales y futuros del otorgante.

4. Alcance del poder:

X Confiero expresamente al apoderado todas las facultades legales para que represente mi(s) interés(es) en la(s) actuación(es) señalada(s) en el punto 3 de este documento, incluyendo:

- ✓ Desistir de la(s) solicitud(es) y de las demás actuaciones.
- ✓ Renunciar a los derechos del registro de signos distintivos o de nuevas creaciones.
- ✓ Sustituir en los mismos términos en que aquí se le confiere el presente poder.
- ✓ Transigir.
- ✓ Recibir.
- ✓ Conciliar
- ✓ Interponer recursos.
- ✓ Contestar oposiciones.

5. Firma:	
DAVID LEONARDO HURTADO	David L Hurtado
Nombre del firmante	
94.552.179 de Cali	
Cédula de Ciudadanía	FIRMA

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference CM-2012-6986	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No **PCT/SG2013/000006**	International filing date *(day/month/year)* 04 January 2013	(Earliest) Priority Date *(day/month/year)* 06 January 2012

Applicant

SMART HUB PTE. LTD

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **4** sheets.

[ ] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

[X] The international application in the language in which it was filed.

[ ] A translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II).

3. [ ] **Unity of invention is lacking** (See Box No. III).

4. With regard to the **title**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

[X] the text is approved as submitted by the applicant.

[ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**.

a. the figure of the **drawings** to be published with the abstract is Figure No. **2**

[X] as suggested by the applicant.

[ ] as selected by this Authority, because the applicant failed to suggest a figure.

[ ] as selected by this Authority, because this figure better characterizes the invention.

b. [ ] none of the figures is to be published with the abstract.

A6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2013/000006

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 (2013.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC: Keywords (TRANSACTION, COMMUNICATION, MOBILE, CARD, LOCK, UNLOCK, ACCOUNT, ENABLE, CHANNEL) and like terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 March 2013	18 March 2013
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au Facsimile No.: (61 2 6283 7999	Vivek Joshi AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0399359616

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation)	DOCUMENTS CONSIDERED TO BE RELEVANT	PCT/SG2013/000006

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7383988 B2 (SLONECKER, Jr.) 10 June 2008 Abstract, Figure 1, 3, Summary of the Invention, Column 8 Lines 60-66 and Column 9 Lines 4-8, 21-53.	1 - 17

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. PCT/SG2013/000006

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 7383988 B2	10 Jun 2008	EP 1934866 A2	25 Jun 2008
		US 2007045403 A1	01 Mar 2007
		US 7383988 B2	10 Jun 2008
		WO 2007027791 A2	08 Mar 2007

End of Annex

US 20070045403A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0045403 A1

Slonecker, JR. (43) Pub. Date: Mar. 1, 2007

(54) SYSTEM AND METHOD FOR LOCKING AND UNLOCKING A FINANCIAL ACCOUNT CARD

(76) Inventor: David B. Slonecker JR., Rosendale, WI (US)

Correspondence Address:
REINHART BOERNER VAN DEUREN S.C.
ATTN: LINDA KASULKE, DOCKET COORDINATOR
1000 NORTH WATER STREET
SUITE 2100
MILWAUKEE, WI 53202 (US)

(21) Appl. No.: 11/217,018

(22) Filed: Aug. 31, 2005

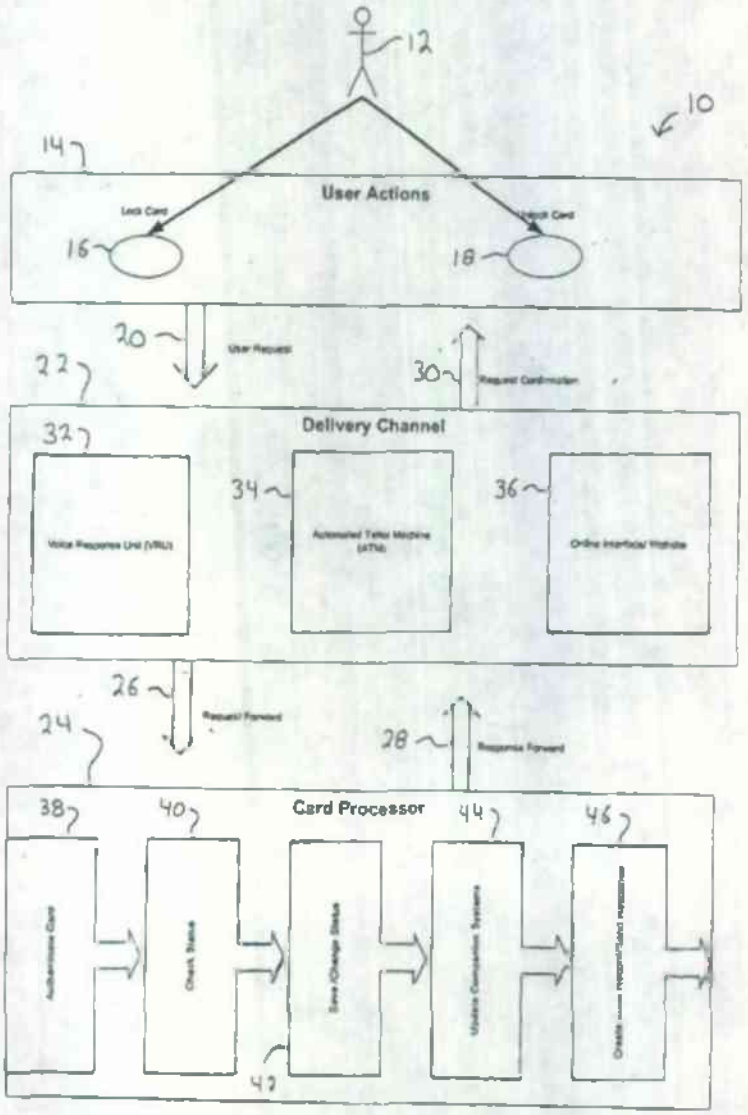
Publication Classification

(51) Int. Cl.
G06K 5/00 (2006.01)

(52) U.S. Cl. 235/380

(57) ABSTRACT

A system and method whereby a holder of a financial account card, such as a credit card or debit card, is able to disable and re-enable use of the card by locking and unlocking the card repeatedly. A request to lock or unlock a card may be provided by a variety of delivery channels, e.g., telephone, automated teller machine, or online, to a card processor. For a locking transaction the card processor saves the current operable status of the card and changes the status to locked. For an unlocking transaction the saved operable status of the card is restored. The changed locked or unlocked status of the card is reported by the card processor to companion systems and an audit record created.



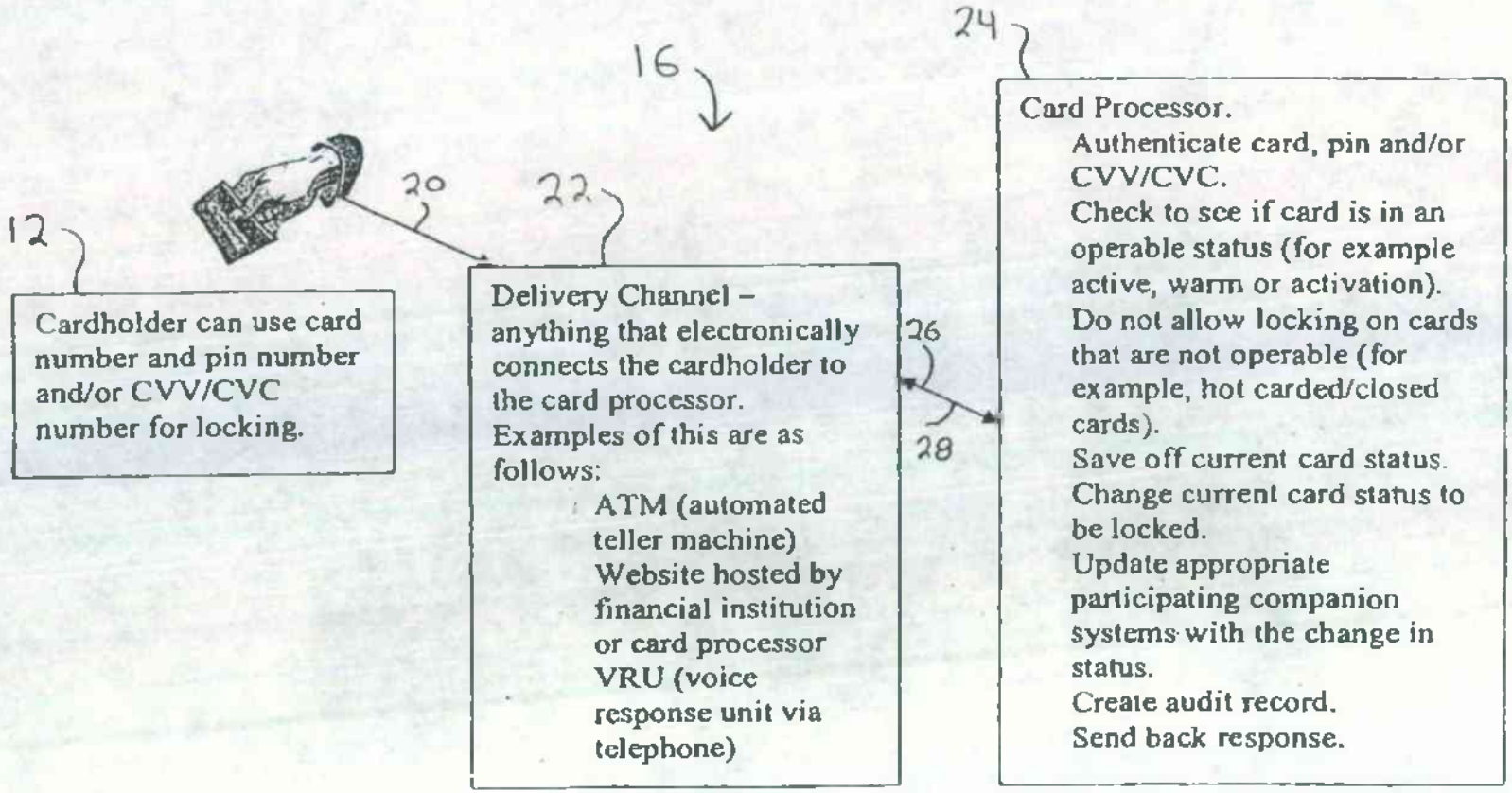

16
24
Card Processor.
Authenticate card, pin and/or CVV/CVC.
Check to see if card is in an operable status (for example active, warm or activation).
Do not allow locking on cards that are not operable (for example, hot carded/closed cards).
Save off current card status.
Change current card status to be locked.
Update appropriate participating companion systems with the change in status.
Create audit record.
Send back response.
20
22
12
Cardholder can use card number and pin number and/or CVV/CVC number for locking.
Delivery Channel – anything that electronically connects the cardholder to the card processor.
Examples of this are as follows:
ATM (automated teller machine)
Website hosted by financial institution or card processor
VRU (voice response unit via telephone)
26
28

Fig. 2

12

Cardholder can use card number and pin number and/or CVV/CVC number for unlocking.

20

22

Delivery Channel – anything that electronically connects the cardholder to the card processor. Examples of this are as follows:

- ATM (automated teller machine)
- Website hosted by financial institution or card processor
- VRU (voice response unit via telephone)

26

28

24

Card Processor.

- Authenticate card, pin and/or CVV/CVC.
- Check to see if card is in locked status. Do not allow unlocking on any status other than locked.
- Move saved off card status (from lock transaction) to current card status.
- Update appropriate participating companion systems with the change in card status.
- Create audit record.
- Send back response.

18

Fig. 4

SYSTEM AND METHOD FOR LOCKING AND UNLOCKING A FINANCIAL ACCOUNT CARD

FIELD OF THE INVENTION

[0001] The present invention pertains generally to financial accounts, such as credit and deposit accounts, and to computer based systems and methods for managing such accounts and, more particularly, to computer implemented systems and methods for managing financial accounts that are accessed by the owners thereof using a card, such as a credit card or a debit card, and to systems and methods for activating and deactivating such cards.

BACKGROUND OF THE INVENTION

[0002] Individuals and businesses typically may hold a variety of financial accounts with a variety of different entities. For example, such financial accounts may include credit accounts, such as credit card accounts, and deposit accounts, such as savings and checking accounts, and the like. Such accounts may be maintained by the owners thereof with a variety of financial institutions, such as banks, savings and loans, credit unions, and other banking entities, as well as with brokerage firms, retail establishments, and the like. The owners of such accounts often may be able to access the accounts via the use of a card, such as a credit card, for accessing a credit account, or a debit card, for accessing a deposit account, such as a savings or checking account. Such cards may be used by the account owner, e.g., to make purchases, by physically presenting the card at a point of purchase. For some transactions, such as mail orders, telephone orders, or orders made over the Internet, the card does not have to be physically present. For such transactions, the credit card number, which typically is physically printed on the card as well as electronically encoded in a magnetic strip on the card that may be read by an appropriate card reader, may be provided to a merchant via mail, over the telephone, and/or via a computer network, e.g., the Internet.

[0003] No matter how the card or card number is presented, the processing of a transaction using the card number typically is performed electronically. The card number is provided electronically to a card processing system, which may or may not be operated by the financial institution or other entity that holds the account being accessed. The card processing system verifies that the card number corresponds to an active account, that the card itself is valid for accessing the account, that account limits have not been exceeded, etc. If the pre-established conditions for accessing the account using the card are satisfied, electronic approval is provided by the processing system to indicate that the card transaction may proceed.

[0004] A variety of security measures may be employed to ensure that a card used for accessing an underlying financial account is used only by the account owner or someone authorized by the account owner. For example, for some card transactions, such as a cash withdrawal or draw on the account from an automatic teller machine (ATM), or at some retail outlets, the individual presenting the card will be required to provide a personal identification number (PIN) that is not printed or otherwise provided on the card itself. An individual presenting a card for a transaction may be required to provide a signature on the transaction receipt. This signature is compared to a signature on the card by a person conducting the transaction to verify that the card owner and person presenting the card are the same individual. Some credit cards and debit cards may have a photograph of the card owner thereon, which also can be used to verify that the person presenting the card is the card owner. Some credit card transactions, particularly credit card transactions performed online over the internet, may require the card user to provide a card verification value (CVV) or card verification code (CVC) as an additional security measure. The CVV/CVC are numeric codes constructed by a cryptographic process based on card data, such as the card number, the expiration date, etc., that are written to the magnetic stripe of the card as well as printed on the back of the card. Merchants and others who accept credit cards, debit cards, and the like for payment employ these and other methods to prevent use of such cards by those who are not authorized to do so.

[0005] Despite the security measures mentioned above, when a financial account card, such as a credit card or debit card, is lost or stolen there is still significant risk that the card may be used and, therefore, the underlying financial account accessed, by an unauthorized person. Thus, financial account card issuers strongly recommend that, if a card is lost, stolen, or otherwise misplaced, the card owner immediately contact the card issuer. Card issuers conveniently provide a toll-free customer service telephone number that may be called at any time by a card holder in the event that a card is lost, stolen, or misplaced. Upon calling the customer service number the card owner will be asked to provide the card number or account number for the card that was lost or stolen or misplaced. This number will be entered into the card processing system electronically, and the card will automatically be cancelled or disabled. That is, no further transactions using the cancelled card number will be allowed by the card processing system. If any attempt is made to use the card number or a card bearing the card number after the card is cancelled in this manner, the card processing system will reject the transaction, providing an indication that the card is no longer valid or has been cancelled. Typically, upon canceling a financial account card in this manner, the credit card processing system will automatically initiate a process to issue to the card owner a new replacement card bearing a new card number, such that the card owner may be able to access the underlying financial account using the new card number.

[0006] A misplaced credit or debit card can cause a card owner considerable anxiety. A missing card may be in the hands of someone who may try to use the card or card number to access the owner's financial accounts. Thus, it is quite reasonable to want to cancel a financial account card as soon as it turns up missing. However, canceling a credit or debit card can be inconvenient. Once the card is cancelled, the card owner must do without the card, and may not have access to the underlying account, until a new card is received. This could take several days or even longer. Furthermore, the card owner may have established future automatic and/or recurring charges to be made to the card number. Once a financial account card is cancelled, the old card number is no longer valid, and any such pre-established charges to the cancelled card number will be rejected. Thus, the card owner may have to contact various merchants or others to change the card number to be used when the new card and card number is received. All of these inconve-

23

[0017] FIG. **5** is a more detailed flow chart diagram of an exemplary method for unlocking a financial account card in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] An exemplary system **10** and method for locking and unlocking a financial account card in accordance with the present invention will be described in detail herein first with reference to FIG. **1**. Based on the detailed written description of the functionality of a system in accordance with the present invention, along with the detailed flow chart diagrams and other illustrations, presented herein, a person of ordinary skill in the art of computer programming for the processing of financial accounts will be able to implement a system and method for locking and unlocking a financial account card in accordance with the present invention on conventional and future computer based systems running conventional operating systems and using conventional programming language and techniques. For example, the present invention may be implemented as part of conventional present or future computer based systems for processing financial account cards and financial account card transactions.

[0019] The present invention may be applied to the locking and unlocking of any financial account card that may be owned by an individual or business card owner **12**. For example, the present invention may be applied to credit cards, debit cards, or other account cards as issued by financial institutions and other card issuers. Such cards may provide access to underlying credit accounts, deposit accounts (such as checking and savings accounts), brokerage accounts, or any other type of financial account as may be held by a financial institution (bank, savings and loan, credit union), brokerage firm, retail or other business or any other entity.

[0020] In accordance with the present invention, a card owner **12** is able to perform alternatively two user actions **14** related to a financial account card. The card owner **12** may either lock the card **16**, thereby preventing use of the card and preventing access to the underlying account using the card number, or unlock the card **18**, thereby allowing use of the card and access to the underlying account using a previously locked card number.

[0021] The card owner **12** initiates a user action **14**, either locking **16** or unlocking **18** a card, by providing a user request **20** via a delivery channel **22** to a card processor **24**. As will be discussed in more detail below, a variety of different delivery channels **22** may be made available to the card owner **12**. The delivery channels forward **26** a user request **20** for a user action **14**, to lock **16** or unlock **18** a card, to the card processor **24**. The card processor **24** may generate and forward a response **28** indicating that a user request has been received and whether or not the requested user action **14** has been implemented by the card processor **24**. This response **28** is delivered via the selected delivery channel **22** as a user action request confirmation **30** to the card owner **12**.

[0022] In accordance with the present invention, a variety of delivery channels **22** may provide a user interface for a card owner **12** to present a request to lock **16** or unlock **18** a financial account card to the card processor **24**, wherein the locking or unlocking operation is implemented. Exemplary delivery channels **22** that may be employed in accordance with the present invention for this purpose include: a telephone system using a voice response unit (VRU) interface **32**, an automated teller machine (ATM) **34** interface, and/or an online interface **36** via a computer network such as the internet. It should be understood that other similar or different current or future delivery channels may be employed in accordance with the present invention to provide a user interface between the card owner **12** and the card processor **24**. Any such delivery channel **22** employed in accordance with the present invention preferably provides an electronic connection between the card owner **12** and the card processor **24**. A delivery channel **22** requiring human intervention may be employed in accordance with the present invention. For example, the delivery channel **22** may include a human operator at a customer service center. In such case, the card owner **12** may call the customer service center and present the request to a live person that a financial account card be locked **16** or unlocked **18**. The live operator may then respond to the card owner's **12** request by entering the request, along with appropriate card owner identification, as will be discussed in more detail below, into the card processor system **24** via an appropriate connection thereto, e.g., via a computer network.

[0023] A card owner **12** may provide a user action **14** request **20** to a card processor **24** via a VRU **32** delivery channel **22** by calling an appropriate telephone number provided to the card owner. Such a number preferably is provided to the card owner **12** along with other account information provided to the card owner **12** at the time that the card is issued, and preferably also may be printed on the card as well as provided on monthly account statements. A recorded and/or computer generated voice provided by the VRU **32** may prompt the card owner **12** to enter appropriate card identification information, such as the card number, and other confirming information, such as a personal identification number (PIN) and/or a card verification value (CVV) or card verification code (CVC). Such numerical information may be entered into the VRU **32** by the card owner **12** using the keys of a touch tone phone with which the card owner **12** is calling the VRU **32**. Alternatively, a voice recognition unit implemented as part of the VRU **32** may be employed to allow the card owner **12** merely to speak the required information into the telephone. Similarly, the card owner **12** may be prompted to indicate the user action **14** being requested, i.e., either to lock **16** or unlock **18** the financial account card identified. The identification and user action information entered by the card owner **12** via the VRU **32** is then forwarded **26** to the card processor **24** for implementation, e.g., by an appropriate computer network connection. A response **28** confirming **30** that the user action request has been forwarded to the card processor **24**, and either implemented or, for some reason, not implemented, may be provided to the card owner **12** via the VRU **32** with an appropriate recorded and/or computer generated voice message. Conventional current or future VRUs **32** or similar devices or systems may be used to implement the process just described.

[0024] The card owner **12** may present a request **20** to lock **16** or unlock **18** a financial account card to the card processor **24** via an ATM **34** by providing the card to be locked or unlocked to the ATM **34** in a conventional manner. The card number, and/or other identifying information, may be read

24

stored in a card database **50**, the card processor verifies that the card is authentic **48**. For example, as part of the authentication process **48** it may be determined whether or not the card number corresponds to a valid financial account card that may be processed by the card processor **24** as identified in the card database **50**. The authentication process **48** may also verify that the identifying information (PIN and/or CVV/CVC) as provided correspond with the provided card number. This verifies that the locking transaction **16** is being requested by an authorized card owner **12**. Other card authentication processes also may be performed. For example, if the lock transaction request **16** was received via a VRU **32** delivery channel **22**, it may be determined whether the request came from a phone number associated with the card owner **12**. Similarly, if the lock transaction request **16** was received via an online interface **36** delivery channel **22**, it may be determined whether the request came from a computer associated with the card owner **12**.

[0030] If the card presented to be locked is verified as authentic **48**, the current activation status of the card is checked to verify that the card is operable **52**. Various status flags or codes are associated with each card number and maintained in the card database **50**. The current operable status of the card is determined by the condition of these various status codes or flags. The locking process will not be allowed to proceed if it is determined from the status codes in the card database **50** that the card in question is not in an operable status, e.g., status codes indicate that the card is "hot carded", closed, cancelled, already locked, etc.

[0031] If the card to be locked is determined **52** to be currently operable, the current operable status of the card from the card database **50** is saved **54**. The saved card status may be saved in a separate database **56** and/or as part of the card database **50**.

[0032] Having saved the current active status of the card **54**, the activation status of the card may be changed to a locked status **58**. This change in activation status is recorded in the card database **50**. For example, the locked status of the card may be indicated by setting a status code or flag associated with the card number in the card database **50** to a condition indicating that the card is locked. Preferably a separate code or flag is employed to indicate the locked/unlocked status of the card. That is, the code or flag selected to be used for this purpose is not used for any other purpose, i.e., is not used to indicate any other card activation status.

[0033] Having changed the current status of the card to locked **58** in the card database **50**, the changed card status may be used to update **60** any companion systems **62**. A companion system **62** is any system, other than the card processor system **24** that houses the locked/unlocked status of a financial account card, that needs to or should know the status of the card. For example, the card processor **24** may be the main processor that is supposed to receive authorization requests for card transactions. However, in some cases, a companion system **62** in front of the card processor **24** may stand in for the card processor **24** and make the authorization decision without passing the request to the card processor **24**. For example, if the card processor **24** is not responding to an authorization request, a companion system **62** may be authorized to perform the authorization based on pre-established criteria. Some financial account card issuers may want a companion system **62** to authorize transactions that are under a certain floor limit (such as $5) instead of going out to the main card processor **24** to perform the authorization. In such cases the current locked or unlocked status of the card as established by the card processor **24** should be made available to the companion system **62**, because the companion system **62** should have available the latest status of the card in making authorization decisions. In other words, the companion system **62** must know the card status so that transactions are not authorized for locked cards. Thus, the locked condition of the card is distributed such that, when locked, use of the card to perform any transactions (other than an unlock transaction **18**) is prevented. Communication between the card processor **24** and any companion systems **62** to perform such status updates **60** may employ any means of electrical communications between systems, such as a computer network.

[0034] An audit record **64** of the requested locking transaction **16** then may be saved in an appropriate database **66**. The audit record created **64** may include such information as the card number, when the lock transaction **16** was requested, whether or not the lock transaction **16** was successfully implemented, etc. If the card was not appropriately authenticated **48** or found inoperable **52**, and, therefore, the lock transaction **16** could not be implemented, this information also preferably may be stored in the audit record database **66**. The audit record database **66** may be employed by an operator of the card processor system **24** to perform various statistical analyses, e.g., on who is requesting card locks, the number of card locking transactions **16** requested by each card owner **12**, etc.

[0035] Finally, a response **68** may be generated and sent back to the customer card owner **12**, via the selected delivery channel **22**. The response sent **68** to the customer card owner **12** may confirm that the lock transaction **16** request has been received, whether or not the requested lock transaction **16** has been implemented, and, if not implemented, may indicate why the lock transaction **16** was not implemented (card not identified as authentic, card already locked, etc.). This ends **70** the card locking transaction **16**.

[0036] An exemplary card unlocking transaction **18** as implemented by a system and method in accordance with the present invention now will be described in overview first with reference to FIG. **4**. As with the card locking transaction **16**, the card owner **12** initiates the card unlocking transaction **18** by providing the number of the financial account card to be unlocked and other requested identifying information, e.g., a PIN and/or CVV/CVC number, via a selected delivery channel, e.g., VRU **32**, ATM **34**, or online **36**. In this case, however, the card owner **12** requests **20** that the card be unlocked **18**. The card unlocking transaction request **20**, along with the card number and other identifying information, is forwarded **26** via the selected delivery channel **22** to the card processor **24** for implementation. A response **28** may be sent back from the card processor **24**, via the selected delivery channel **22**, to the card owner **12**, to indicate that the card unlocking operation request has been received and has, or has not, been implemented.

25

8. The system of claim 7 wherein the card processor is adapted to unlock the card by setting the locked/unlocked status code to an unlocked state.

9. The system of claim 1 wherein the card processor is adapted to send a message to at least one companion system informing the at least one companion system that the card has been locked or unlocked.

10. The system of claim 1 wherein the card processor is adapted to save an audit record of a requested card lock operation and of a requested card unlock operation.

11. A method implemented in a computer system of locking and unlocking a financial account card, comprising:

(a) receiving card identifying information and a request to perform a card lock operation or a request to perform a card unlock operation via a delivery channel;

(b) authenticating the card identifying information;

(c) in response to a request to perform a card lock operation

(i) verifying that the card to be locked currently is in an operable state;

(ii) saving the operable state of the card;

(iii) locking the card by changing the current state of the card to a locked state whereby use of the card is prevented;

(d) in response to a request to perform a card unlock operation

(iv) verifying that the card to be unlocked currently is in a locked state;

(v) retrieving the saved operable state of the card;

(vi) unlocking the card by changing the current state of the card to the retrieved saved operable state of the card; and

(e) sending a response message via the delivery channel indicating that the request to perform a card lock operation or the request to perform a card unlock operation has been received.

12. The method of claim 11 wherein the delivery channel is selected from the group of delivery channels consisting of a voice response unit (VRU), an automated teller machine (ATM), and a computer network online interface.

13. The method of claim 11 wherein the card identifying information includes a card number and other identifying information.

14. The method of claim 13 wherein the other identifying information is selected from the group of identifying information consisting of a personal identification number (PIN), a card verification value (CVV), and a card verification code (CVC).

15. The method of claim 13 wherein authenticating the card identifying information includes verifying that the received card number corresponds to the received other identifying information.

16. The method of claim 11 wherein the card identifying information identifies a financial account card selected from the group of financial account cards consisting of credit cards and debit cards.

17. The method of claim 11 wherein locking the card includes setting a locked/unlocked status code associated with the card number to a locked state and wherein the locked/unlocked status code is used only to indicate whether the card is locked or unlocked.

18. The method of claim 17 wherein unlocking the card includes setting the locked/unlocked status code to an unlocked state.

19. The method of claim 11 comprising additionally sending a message to at least one companion system informing the at least one companion system that the card has been locked or unlocked.

20. The method of claim 11 comprising additionally saving in a database an audit record of a requested card lock operation and of a requested card unlock operation.

21. A method of locking and unlocking a financial account card, comprising:

(a) providing a card processor implemented in a computer system, coupled to a delivery channel, and adapted to receive card identifying information, a request to perform a card lock operation, and a request to perform a card unlock operation via the delivery channel, to authenticate the card identifying information, in response to a request to perform a card lock operation to

(i) verify that the card to be locked currently is in an operable state;

(ii) save the operable state of the card;

(iii) lock the card by changing the current state of the card to a locked state whereby use of the card is prevented; and

in response to a request to perform a card unlock operation to

(iv) verify that the card to be unlocked currently is in a locked state;

(v) retrieve the saved operable state of the card;

(vi) unlock the card by changing the current state of the card to the retrieved saved operable state of the card;

(b) requesting via a delivery channel that a card lock operation be performed by the card processor for a particular identified card;

(c) requesting via a delivery channel that a card unlock operation be performed by the card processor for the particular identified card; and

(d) making the requests of (b) and (c) in sequence repeatedly a plurality of times.

22. The method of claim 21 wherein the card processor is coupled to a plurality of different delivery channels and wherein requesting that a card lock operation be performed and requesting that a card unlock operation be performed are made via different delivery channels.

* * * * *

26

CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS

CONTENIDO

CAPITULO DÉCIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS

1. Ámbito de aplicación

Las instrucciones de que trata el presente capitulo deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), con excepción de las siguientes: el Fondo de Garantías de Instituciones Financieras "Fogafín", el Fondo de Garantías de Entidades Cooperativas "Fogacoop", el Fondo Nacional de Garantías S.A. "F.N.G. S.A.", el Fondo Financiero de Proyectos de Desarrollo "Fonade", los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado público de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación.

Sin embargo, las entidades exceptuadas de la aplicación del presente capítulo citadas en el párrafo anterior, deberán dar cumplimiento a los criterios de seguridad y calidad de la información, establecidos en los numerales 2.1. y 2.2 del presente capítulo.

El numeral 3.1.13 "Elaborar el perfil de las costumbres transacciones de cada uno de sus clientes ..." deberá ser aplicado únicamente por los establecimientos de crédito, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

El numeral 7 "Análisis de vulnerabilidades" deberá ser aplicado únicamente por los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

Los establecimientos de crédito que presten servicios financieros a través de corresponsales no bancarios deberán sujetarse, para el uso de este canal de distribución, a las instrucciones contenidas en el capítulo noveno, Título III de la presente circular.

En todo caso las entidades vigiladas destinatarias de las instrucciones del presente numeral, deberán implementar los requerimientos exigidos atendiendo la naturaleza, objeto social y demás características particulares de su actividad.

2. Definiciones y criterios de seguridad y calidad

Para el cumplimiento de los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales y medios de distribución de productos y servicios para clientes y usuarios, las entidades deberán tener en cuenta las siguientes definiciones y criterios:

2.1. Criterios de Seguridad de la Información

a) **Confidencialidad**: Hace referencia a la protección de información cuya divulgación no está autorizada.

b) **Integridad**: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

c) **Disponibilidad**: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

2.2. Criterios de Calidad de la información

a) **Efectividad**: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

b) **Eficiencia**: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

c) **Confiabilidad**: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

2.3. Canales de distribución de servicios financieros

Para los efectos del presente capítulo son canales de distribución de servicios financieros los siguientes:

a) Oficinas.
b) Cajeros Automáticos (ATM).
c) Receptores de cheques
d) Receptores de dinero en efectivo
e) POS (incluye PIN Pad).
f) Sistemas de Audio Respuesta (IVR).
g) Centro de atención telefónica (Call Center, Contact Center).
h) Sistemas de acceso remoto para clientes (RAS).
i) Internet.
j) Dispositivos móviles.

2.4. Medios

Son instrumentos que permiten la realización de operaciones a través de los canales de distribución descritos en el numeral anterior, tales como: cheques, tarjetas débito y crédito, dinero.

2.5. Vulnerabilidad Informática

Ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistema específico de forma no autorizada y emplearlo en beneficio propio o como origen de ataques por parte de terceros.

2.6. Cifrado fuerte

Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES.

2.7. Sistema de Acceso Remoto (RAS)

Para efectos de la presente circular, RAS hace referencia a la conexión realizada por un tercero a los sistemas de información de la entidad utilizando enlaces dedicados o conmutados.

2.8. Operaciones

Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que prestan las entidades a sus clientes o usuarios p. ej., consulta de saldo, cambio de clave, actualización de datos, etc. Cuando la operación implique o conlleve movimiento de dinero se denominará transacción, p. ej., retiros, transferencias, depósitos, pagos, corrección y consultas de historias laborales, etc.

2.9. Cliente

Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.

2.10. Usuario

Aquella persona natural o jurídica a la que, sin ser cliente, la entidad le presta un servicio.

2.11. Producto

Son las operaciones legalmente autorizadas que pueden adelantar las entidades vigiladas mediante la celebración de un contrato (V. gr. cuenta corriente o de ahorros, seguros, inversiones, CDT, giros, cuentas de ahorro pensionales y de cesantías, etc.).

2.12. Servicio

Es toda aquella interacción de las entidades sometidas a inspección y vigilancia de la SFC con sus clientes y usuarios para el desarrollo de su objeto social.

2.13. Dispositivo

Mecanismo, máquina o aparato dispuesto para producir una función determinada.

2.14. Información confidencial

Atendiendo lo dispuesto en el artículo 15 de la Constitución Política de Colombia y sin perjuicio de lo establecido en el numeral 4 Capítulo Noveno de la presente Circular y demás normas aplicables sobre la materia, se considerará confidencial para efectos de la aplicación del presente Capítulo toda aquella información amparada por la reserva bancaria V. gr. número de cuenta; número de identificación personal (PIN); número de tarjeta física; información sobre depósitos o inversiones de cualquier tipo, créditos, saldos, cupos y movimientos de cuenta, siempre que vayan acompañados del nombre o número de identificación del cliente.

Las entidades podrán clasificar como confidencial otro tipo de información. Esta clasificación deberá estar debidamente documentada y a disposición de la Superintendencia Financiera de Colombia.

3. Obligaciones Generales

En desarrollo de lo dispuesto en el presente Capítulo, las entidades deberán incluir en sus políticas y procedimientos relativos a la administración de la información, los criterios de que tratan los numerales 2.1 y 2.2.

Adicionalmente, para dar aplicación a dichos criterios las entidades deberán adoptar, al menos, las medidas que se relacionan a continuación:

3.1. Seguridad y Calidad

En desarrollo de los criterios de seguridad y calidad, y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

3.1.1. Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.

3.1.2. Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible.

3.1.3. Disponer que el envío de información a sus clientes, tales como certificaciones, extractos, notificaciones, sobreflex, entre otros, así como los medios (tarjetas débito y crédito, chequeras, etc.) se haga en condiciones de seguridad. Cuando la información que la entidad remite a sus clientes sea de carácter confidencial y se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.

3.1.4. Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

3.1.5. Velar por que la información enviada a los clientes esté libre de software malicioso.

3.1.6. Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.

3.1.7. Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

3.1.8. Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.

3.1.9. Disponer de los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales se les prestará servicios por los diferentes canales, dejando constancia de ello. En desarrollo de lo anterior, la entidad deberá permitir que el cliente, por lo menos, inscriba las cuentas a las cuales realizará transferencias o pagos, defina montos, número de operaciones y canales. En cualquier caso, los montos máximos deberán ser definidos por la entidad. Así mismo, deberá permitir que el cliente registre las direcciones IP, los números de los teléfonos fijos y móviles desde los cuales operará. La entidad podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.

3.1.10. Ofrecer, cuando el cliente así lo exija, la posibilidad de manejar una contraseña diferente para cada uno de los canales.

3.1.11. Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

3.1.12. Establecer procedimientos para el bloqueo de canales o de medios, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.

3.1.13. Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación de las operaciones que no correspondan a sus hábitos.

3.1.14. Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales y medios de servicio al cliente y al usuario. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

3.1.15. Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.

3.1.16. Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

3.1.17. Tener en operación solo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

3.1.18. Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

3.1.19. Incluir en el informe de gestión a que se refiere el artículo 47 de la ley 222 de 1995 y sus modificaciones, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.

3.1.20. Considerar en sus políticas y procedimiento relativos a los canales y medios de distribución de productos y servicios, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.

3.2. Tercerización – Outsourcing

Las entidades que contraten bajo la modalidad de *outsourcing* o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información confidencial de la entidad o de sus clientes, deberán cumplir, como mínimo, con los siguientes requerimientos:

3.2.1. Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.

3.2.2. Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capítulo, por lo menos, los siguientes aspectos:

a) Niveles de servicio y operación.
b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
c) Propiedad de la información.
d) Restricciones sobre el software empleado.
e) Normas de seguridad informática y física a ser aplicadas.
f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

3.2.3. Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas.

3.2.4. Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados.

3.2.5. Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.

3.3. Documentación

En materia de documentación las entidades deben cumplir, como mínimo, con los siguientes requerimientos:

3.3.1. Dejar constancia de todas las operaciones que se realicen a través de los distintos canales de distribución de servicios para clientes y usuarios que contenga por lo menos lo siguiente: fecha, hora, código del equipo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión) número de la operación, cuenta(s), costo de la misma para el usuario.

3.3.2. Velar por que los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las normas vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los diferentes canales de distribución.

3.3.3. Mantener a disposición de la SFC estadísticas anuales con corte a 31 de diciembre de cada año respecto de la prestación de servicios a través de cada uno de los canales de distribución, que contemplen: el número de operaciones realizadas y el nivel de disponibilidad del canal. Esta información deberá ser conservada por un término de tres (3) años.

3.3.4. Cuando a través de los distintos canales se pidan y se realicen donaciones, se deberá generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.

3.3.5. Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

3.3.6. Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.

3.3.7. Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

3.3.8. Dejar constancia del cumplimiento de la obligación establecida en el numeral 3.4.4.

3.3.9. Grabar las llamadas realizadas por los clientes a los centros de atención telefónica que conlleven a la consulta o actualización de su información.

3.3.10. La información a que se refieren los numeral 3.3.1, 3.3.6 y 3.3.9 deberá ser conservada por lo menos por dos (2) años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

3.4. Divulgación de Información

En materia de divulgación de información las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

3.4.1. En concordancia con lo dispuesto en el artículo 97 del E.O.S.F., suministrar a los clientes información clara, completa y oportuna de los productos, servicios y operaciones.

3.4.2. Dar a conocer a sus clientes y usuarios, por el respectivo canal y en forma previa a la realización de la operación, el costo de la misma, si lo hay, brindándoles la posibilidad de efectuarla o no. Tratándose de cajeros automáticos la obligación solo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia.

3.4.3. Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.

3.4.4. Informar y capacitar a los clientes acerca de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

3.4.5. Establecer y publicar por los canales de distribución, en los que sea posible, las medidas de seguridad que deberá adoptar el cliente para el uso de los mismos.

3.4.6. Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales.

3.4.7. Expedir un soporte, en papel o por medios electrónicos, al momento de la realización de cada transacción. Dicho soporte deberá contener al menos la siguiente información: fecha, hora (hora y minuto), código del equipo (para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles: el número desde el cual se hizo la conexión), número, costo de la operación para el cliente o usuario, tipo, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan la operación. Se deberán ocultar los números de las cuentas con excepción de los últimos cuatro (4) caracteres, salvo cuando se trate de la cuenta que recibe una transferencia. Cuando no se pueda entregar el soporte, se deberá advertir previamente al cliente o usuario de esta situación. Para el caso de IVR se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la transacción. En relación con el costo de la operación y tratándose de cajeros automáticos la obligación solo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia.

3.4.8. Entregar constancia, dentro del procedimiento de cancelación solicitado por el cliente, de un producto, en la que se advierta encontrarse a paz y salvo por todo concepto, asegurándose que los futuros reportes a las centrales de riesgo sean consistentes con su estado de cuenta. Tratándose de tarjetas de crédito dicha constancia deberá entregarse al cliente en un tiempo máximo de cuarenta y cinco (45) días, contados a partir de la fecha de solicitud de la cancelación.

4. Obligaciones Adicionales por Tipo de Canal

4.1. Oficinas

Para las oficinas donde se realicen transacciones las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

4.1.1. Los sistemas informáticos empleados para la prestación de servicios en las oficinas deben contar con soporte por parte del fabricante o proveedor.

4.1.2. Los sistemas operacionales de los equipos empleados en las oficinas deben cumplir al menos con el nivel de seguridad C2 (protección de acceso controlado).

4.1.3. Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deberán ser conservadas por lo menos un (1) año o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.1.4. Disponer de los mecanismos necesarios para evitar que personas no autorizadas atiendan a los clientes o usuarios en nombre de la entidad.

4.1.5. La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito especifico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

4.1.6. Establecer procedimientos necesarios para atender de manera segura y eficiente a sus clientes en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios, fechas y horas de mayor congestión, posible alteración del orden público, entre otras, así como para el retorno a la normalidad. Las medidas adoptadas deberán ser informadas oportunamente a los clientes y usuarios.

4.1.7. Contar con los elementos necesarios para la debida atención del público, tales como: lectores de código de barras, contadores de billetes y monedas, PIN Pad, entre otros, que cumplan con las condiciones de seguridad y calidad, de acuerdo con los productos y servicios ofrecidos en cada oficina.

4.2. Cajeros Automáticos (ATM)

Los cajeros automáticos deberán cumplir, como mínimo, con los siguientes requerimientos:

4.2.1. Contar con sistemas de video grabación que asocien los datos y las imágenes de cada transacción. Las imágenes deberán ser conservadas por lo menos un (1) año o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.2.2. Cuando el cajero automático no se encuentre físicamente conectado a una oficina, la información que viaja entre este y su respectivo sitio central de procesamiento se deberá proteger utilizando cifrado fuerte, empleando para ello hardware de propósito específico independiente. Las entidades deberán evaluar con regularidad la efectividad y vigencia del mecanismo de cifrado adoptado.

4.2.3. Los dispositivos utilizados para la autenticación del cliente o usuario en el cajero deben emplear cifrado.

4.2.4. Implementar el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas.

4.2.5. Los sitios donde se instalen los cajeros automáticos deberán contar con las medidas de seguridad físicas para su operación y estar acordes con las especificaciones del fabricante. Adicionalmente, deben tener mecanismos que garanticen la privacidad en la realización de transacciones para que la información usada en ellas no quede a la vista de terceros.

4.2.6. Implementar mecanismos de autenticación que permitan confirmar que el cajero es un equipo autorizado dentro de la red de la entidad.

4.3. Receptores de Cheques

Los dispositivos electrónicos que permitan la recepción o consignación de cheques deberán cumplir, como mínimo, con los siguientes requerimientos:

4.3.1. Contar con mecanismos que identifiquen y acepten los cheques, leyendo automáticamente, al menos, los siguientes datos: la entidad emisora, el número de cuenta y el número de cheque.

4.3.2. Los cheques o documentos no aceptados por el módulo para recepción de cheques no podrán ser retenidos y deberán ser retornados inmediatamente al cliente o usuario, informando la causa del reintegro.

4.3.3. Una vez el cliente o usuario deposite el cheque, el sistema deberá mostrar una imagen del mismo y la información asociada a la transacción, para confirmar los datos de la misma y proceder o no a su realización. En caso negativo deberá devolver el cheque o documento, dejando un registro de la operación.

4.3.4. Como parte del procedimiento de consignación del cheque se le debe poner una marca que indique que este fue depositado en el módulo.

4.4. Receptores de Dinero en Efectivo

Los dispositivos que permitan la recepción de dinero en efectivo deberán cumplir, como mínimo, con los siguientes requerimientos:

4.4.1. Contar con mecanismos que verifiquen la autenticidad y denominación de los billetes.
4.4.2. Totalizar el monto de la operación con los billetes aceptados y permitir que el cliente o usuario confirme o no su realización. En este último caso se debe devolver la totalidad de los billetes entregados, generando el respectivo registro.
4.4.3. Las operaciones en efectivo deben realizarse en línea, afectando el saldo de la respectiva cuenta. La operación no quedará sujeta a verificación.
4.4.4. Los billetes no aceptados no podrán ser retenidos y deben ser retornados inmediatamente al cliente o usuario.

4.5. POS (Incluye PIN Pad)

Los POS deberán cumplir, como mínimo, con los siguientes requerimientos:

4.5.1. La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad.
4.5.2. Cumplir el estándar EMV (Europay, MasterCard, VISA).
4.5.3. Los administradores de las redes de este canal deberán validar automáticamente la autenticidad del datáfono que se intenta conectar a ellos, así como el medio de comunicación a través del cual operará.
4.5.4. Establecer procedimientos que le permitan a los responsables de los datáfonos en los establecimientos comerciales, confirmar la identidad de los funcionarios autorizados para retirar o hacerle mantenimiento a los equipos.
4.5.5. Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados.
4.5.6. Contar con mecanismos que reduzcan la posibilidad de que terceros puedan ver la clave digitada por el cliente o usuario.

4.6. Sistemas de Audio Respuesta (IVR)

Los sistemas de audio respuesta deberán cumplir, como mínimo, con los siguientes requerimientos:

4.6.1. Permitir al cliente confirmar la información suministrada en la realización de la transacción.
4.6.2. Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público.

4.7. Centro de Atención Telefónica (Call Center, Contact Center)

Los centros de atención telefónica deberán cumplir, como mínimo, con los siguientes requerimientos:

4.7.1. Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.
4.7.2. Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
4.7.3. Dotar a los equipos que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.
4.7.4. Garantizar que los equipos destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.
4.7.5. En los equipos usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos un (1) año o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.8. Sistemas de Acceso Remoto para Clientes

Las entidades que ofrezcan servicio de acceso remoto para la realización de transacciones deberán contar con un módulo de seguridad de hardware para el sistema, que cumpla al menos con el estándar de seguridad FIPS-140-2 (Federal Information Processing Standard), el cual deberá ser de propósito específico (appliance) totalmente separado e independiente de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, de servidores de acceso remoto (RAS) y/o de concentradores.

4.9. Internet

Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir con los siguientes requerimientos:

4.9.1. Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
4.9.2. Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.
4.9.3. Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
4.9.4. Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
4.9.5. Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.
4.9.6. Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

4.10. Prestación de Servicios a través de Nuevos Canales

Cuando la entidad decida iniciar la prestación de servicios a través de nuevos canales, diferentes a los que tiene en uso, además del cumplimiento de las instrucciones generales de seguridad y calidad, deberá adelantar el respectivo análisis de riesgos del nuevo canal. Dicho análisis deberá ser puesto en conocimiento de la junta directiva y los órganos de control.

La entidad deberá remitir a la SFC, con al menos quince (15) días calendario de antelación a la fecha prevista para el inicio de la distribución de servicios a través del nuevo canal, la siguiente información:

a) Descripción del procedimiento que se adoptará para la prestación del servicio.
b) Tecnología que utilizará el nuevo canal.
c) Análisis de riesgos y medidas de seguridad y control del nuevo canal.
d) Planes de contingencia y continuidad para la operación del canal.
e) Plan de capacitación dirigido a los clientes y usuarios, para el uso del nuevo canal, así como para mitigar los riesgos a los que se verían expuestos.

5. Reglas sobre Actualización de Software

Con el propósito de mantener un adecuado control sobre el software, las entidades deberán cumplir, como mínimo, con las siguientes medidas:

5.1. Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.
5.2. Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.
5.3. Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.
5.4. Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.
5.5. Contar con interfases para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.
5.6. Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

6. Obligaciones Específicas por Tipo de Medio – Tarjetas débito y crédito

6.1. Establecer y documentar los procedimientos, controles y medidas de seguridad necesarias para la emisión, transporte, recepción, custodia, entrega, devolución y destrucción de las tarjetas. Se debe estipular el tiempo máximo de permanencia de las tarjetas en cada una de estas etapas.
6.2. Cifrar la información de los clientes que sea remitida a los proveedores y fabricantes de tarjetas, para mantener la confidencialidad de la misma.
6.3. Velar porque los centros de operación en donde se realizan procesos tales como: realce, estampado, grabado y magnetización de las tarjetas, entre otros, así como de la impresión del sobreflex, mantengan procedimientos, controles y medidas de seguridad orientadas a evitar que la información

relacionada pueda ser copiada, modificada o utilizada con fines diferentes a los de la fabricación de la misma.

6.4. Velar porque en los centros donde se realicen los procesos citados en el numeral anterior, apliquen procedimientos y controles que garanticen la destrucción de aquellas tarjetas que no superen las pruebas de calidad establecidas para su elaboración, así como la información de los clientes utilizada durante el proceso. Iguales medidas se deberán aplicar a los sobreflex.

6.5. Establecer los procedimientos, controles y medidas de seguridad necesarias para la creación, asignación y entrega de las claves a los clientes.

6.6. Cuando la clave (PIN) asociada a una tarjeta débito haya sido asignada por la entidad vigilada, esta deberá ser cambiada por el cliente antes de realizar su primera operación.

6.7. Ofrecer a sus clientes mecanismos que brinden la posibilidad inmediata de cambiar la clave de la tarjeta débito en el momento que estos lo consideren necesario.

6.8. Establecer en los convenios que se suscriben con los establecimientos de comercio la obligación de verificar la firma y exigir la presentación del documento de identidad del cliente para las operaciones que se realicen con tarjeta de crédito.

6.9. Emitir tarjetas personalizadas que contengan al menos la siguiente información: nombre del cliente, indicación de si es crédito o débito, nombre de la entidad emisora, fecha de expiración, espacio para la firma del cliente y número telefónico de atención al cliente.

6.10. Al momento de la entrega de la tarjeta a los clientes, ésta deberá estar inactiva. Las entidades deberán definir un procedimiento para su respectiva activación, el cual contemple al menos dos de tres factores de autenticación: algo que se sabe, algo que se tiene, algo que se es. En cualquier caso, se deberán entregar las tarjetas exclusivamente al cliente o a quien este autorice.

6.11. Ofrecer a sus clientes tarjetas débito y/o tarjetas crédito que manejen internamente cualquiera de los mecanismos fuertes de autenticación tales como: OTP (One Time Password), biometría, etc; dichas tarjetas deberán servir indistintamente para realizar transacciones en cajeros automáticos (ATM), en puntos de pago (POS), en Internet y en sistemas de audio respuesta (IVR).

7. Análisis de Vulnerabilidades

Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:

7.1. Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

7.2. Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.

7.3. Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

7.4. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

7.5. Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.

7.6. Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

BANCO INTERNACIONAL

ANEXO AL CONTRATO DE SERVICIOS ELECTRONICOS

AUTORIZACION PARA REALIZAR TRANSACCIONES EN CANALES ELECTRONICOS

Fecha: _____

PERSONA NATURAL / JURIDICA:

Yo, _____ representante legal de (solo persona juridica)

_____ titular de la tarjeta de débito No. _____

autorizo a _____ cargo (solo persona juridica)

_____ No. tarjeta adicional _____.

TRANSACCIONES E INCREMENTO DE CUPOS QUE AUTORIZO REALIZAR:

* Marcar con una X la transacción que desee activar.
* Los montos que constan en este documento, son los que el sistema los asigna automáticamente. Si desea aumentar el cupo diario, por favor indicar el monto requerido.

TRANSACCION	BANCA EN LINEA	CUPO DIARIO ($)	INTERCENTER Telf. 1700-360-360	CAJERO AUTOMATICO	CUPO DIARIO ($)
PAGOS Y COMPRAS:					
Pensión de Colegios		1.000	No disponible		1.000
Tarjeta de Crédito Banco Internacional		3.000	1.000		3.000
Servicios Básicos (Luz /Agua/Teléfono)		300	No disponible		300
Impuestos (Municipales /SRI)		300	No disponible	No disponible	----------
Grupo TVCable		80	No disponible		80
Contecom		----------	No disponible	No disponible	----------
Compra de minutos (Celular)		15	No disponible		Port. 30 - Aleg. 50
Compra de minutos (Internet)		15	No disponible		15
Compra Pasajes Aéreos		300	No disponible		300
TRANSFERENCIAS:					
Incremento Fondo de Inversión		----------	No disponible	No disponible	-
Entre cuentas del cliente		3.000	1.000		1.000
A otras cuentas de clientes del B.I.		3.000	No disponible	No disponible	-
Interbancarios / Pago otras tarjetas de crédito del país		3.000	No disponible	No disponible	-
Al exterior (Monto solicitado por cliente)		*	No disponible	No disponible	-

* Para activar el servicio de transferencias al exterior, se debe adjuntar una carta al Contrato indicando el monto diario y quienes serán los usuarios encargados de ingresar y aprobar las transferencias.

DIRECCIONES DE CORREO ELECTRONICO PARA CONFIRMAR TRANSFERENCIAS E INCREMENTOS EN b@nlnteronline :

1. _____ 2. _____

BLOQUEO DE TRANSACCIONES EN CANALES ELECTRONICOS

* Marcar con una X la transacción que desea bloquear

TRANSACCION	BANCA EN LINEA	TERMINAL DE CONSULTA	INTERCENTER	CAJERO AUTOMATICO
Consulta de productos generales				
Compras				
Pagos				
Solicitudes				
Transferencias				
Otro:				

AUTORIZACION DE SERVICIOS ADICIONALES EN BANCA EN LINEA

Pago a Proveedores	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Pago a Terceros	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Pago de Nómina	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Débito a Terceros	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Pago Instituciones Educativas	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Facturación de Combustible	SI ___	NO ___	*Perfil Usuario: _____	*Código: _____
Relacionar tarjeta adicional para consultar saldos No cuenta (s): _____				

* Para uso interno del Banco

El Cliente

_____
Firma

El Cliente

_____
Firma

Fecha y Firma del responsable del Banco que revisó las cuentas y firmas pertenecientes al cliente.

_____
Firma

Fecha: ____/____/____

Form. 999-1110.10

23.03.09

US 20100312700A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2010/0312700 A1

(43) Pub. Date: Dec. 9, 2010

Coulter et al.

(54) SYSTEM AND METHOD FOR MANAGING STATUS OF A PAYMENT INSTRUMENT

(76) Inventors: **Todd R. Coulter**, Rancho Murieta, CA (US); **Mordechai E. Kaplinsky**, Brooklyn, NY (US); **Christopher E. Lewis**, Tempe, AZ (US); **Jeffery A. Warmington**, Wellington, FL (US)

Correspondence Address:
PERKINS COIE LLP
PATENT-SEA
P.O. BOX 1247
SEATTLE, WA 98111-1247 (US)

(21) Appl. No.: 12/859,205

(22) Filed: Aug. 18, 2010

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/557,457, filed on Sep. 10, 2009.

(60) Provisional application No. 61/112,749, filed on Nov. 8, 2008.

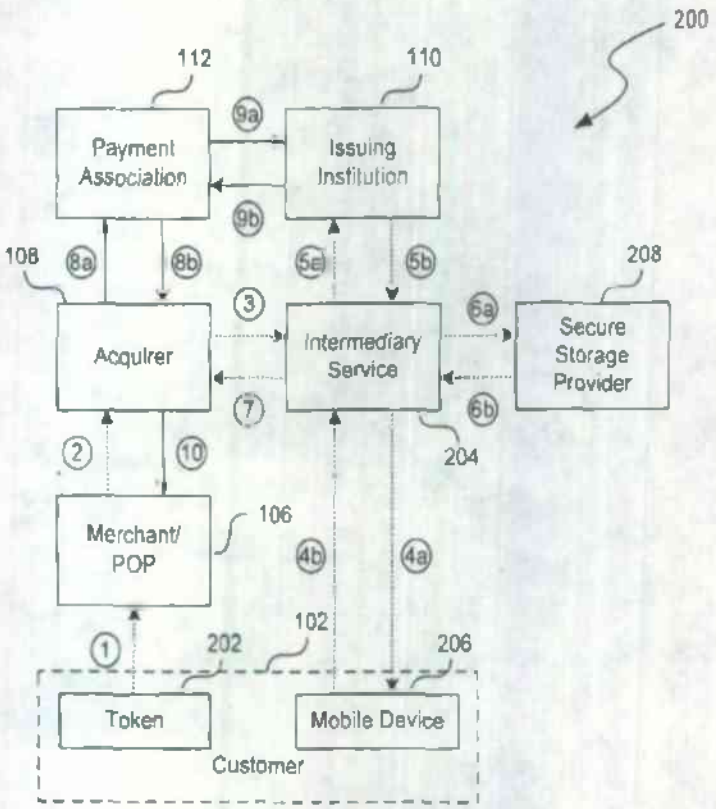
Publication Classification

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

(52) U.S. Cl. 705/42; 705/44

(57) ABSTRACT

A transaction processing service operates as an intermediary between acquirers of financial transaction requests and issuing institutions that process the financial transaction requests. The intermediary service enables a customer to selectively change the status of an account's associated with a payment instrument by activating or deactivating the account. The intermediary service may manage account status locally using a rules module. Alternatively, the issuing institution may manage account status, while the intermediary service provides an interface for customers. A customer communicates with the intermediary service to direct the service to change the account status. The intermediary service determines the account's issuing institution and provides an indication to the issuing institution of the current status of the account (or of the change in status). The intermediary service may provide the indication by transmitting a message to the issuing institution or by storing the account status information in its own database. The issuing institution may then request account status from the intermediary service whenever it needs the information, such as when it receives an authorization request.



initial authorization requests to the intermediary service **204** in lieu of the acquirer forwarding the request. The account information is then returned to the payment association or issuing institution for further processing.

[0121] FIG. **8** illustrates a logical block diagram of the acquirer **108** that implements the process **700** of FIG. **7**. The acquirer **108** redirects certain authorization requests to the intermediary service **204** and generates modified authorization requests based on information provided by the intermediary service **204**. As with the intermediary service **204** shown in FIG. **5**, aspects of the acquirer **108** may be implemented as special-purpose circuitry, programmable circuitry, or as a combination of these. The modules in the acquirer **108** may be implemented in a single physical device or distributed over multiple physical devices and the functionality implemented by calls to remote services.

[0122] As discussed above, the acquirer **108** receives an initial transaction authorization request from the point of purchase **106** and transmits a modified authorization request to the issuing institution **110** via the payment association **112**. The acquirer **108** also communicates with the intermediary service **204** to request account information associated with a particular authorization request and to receive the requested account information. The acquirer **108** also interacts with a storage component **802**, which is configured to store information used to integrate with the intermediary service **204**. In particular, the storage component **802** stores identifying information (such as ranges of account numbers or account number prefixes) that can be used to determine which authorization requests should be handled by the intermediary service **204**. The storage component **802** may also store historical transaction information to be used for auditing or if a transaction is disputed.

[0123] The acquirer **108** includes various modules to assist in processing authorization requests. In particular, the acquirer **108** includes a point of purchase communication module **804**, which is configured to communicate with the point of purchase **106** to receive initial authorization requests and transmit authorization or denial messages at the end of the transaction. The acquirer **108** also includes an evaluation module **806**, which is configured to evaluate initial authorization requests according to the process **700** described above to determine if initial authorization requests should be sent to the intermediary service **204**.

[0124] The acquirer **108** also includes an intermediary service communication module **808**, which is configured to communicate with the intermediary service **204** to send authorization requests and to receive account information. The intermediary service communication module **808** then provides the account information to an authorization request generator module **810**, which is configured to generate a modified authorization request based on the initial authorization request and the received account information. The modified authorization request is then provided to a payment association communication module **812**, which is configured to communicate with the payment association **112** to send the modified authorization requests to the issuing institution **110**. After the issuing institution **110** approves or denies a transaction, the payment association communication module **812** also receives an authorization or denial message from the payment association **112**. The acquirer **108** then forwards the message to the point of purchase **106** and/or the intermediary service **204**.

[0125] One of the advantages of the disclosed intermediary service **204** is that it allows routing of encrypted messages through the service without revealing sensitive information that is contained in the messages to the operator of the service. *FIG. 9 is a block diagram depicting various message routing* paths through the intermediary service **204**. Complementary encryption keys are depicted as being maintained by different parties that participate in the processing of a financial transaction. For example, a key A that is maintained by acquirer **108** *allows the acquirer to encrypt messages and communicate* in a secure fashion with the intermediary service **204**, which maintains a complementary key A' for decoding the encrypted messages. Similarly the intermediary service **204** maintains a key B' that allows it to communicate in a secure fashion *with the mobile device 206, which maintains a* complementary key B. Moreover, the intermediary service **204** also maintains a key C' that allows it to communication in a secure fashion with the issuing institution **110**, which maintains a key C. Of note, however, is the ability of the acquirer **108** and *the issuing institution 110 to exchange encrypted* messages or portions of messages through the intermediary service without allowing the service to read or otherwise act on the contents of the messages. For example, certain portions of the point of purchase information from the initial authori*zation request (e.g., the specific products being purchased)* may be encrypted by the acquirer **108** using an encryption key D. When the intermediary services **204** receives messages or portions of messages that are encrypted, the service copies the encrypted messages or portions of messages and forwards the *copied messages to the issuing institution 110*. The issuing institution **110** is able to decrypt the encrypted message or portion of the message using key D'. Similarly, the issuing institution **110** may encrypt account information using key D so that the information may be read only by the acquirer **108**. *An advantage of this is that the intermediary service* **204** never has usable access to the encrypted information. This allows the acquirer to retain control over non-essential customer information, such as certain point of purchase information, and increases the privacy of the information. It also *allows the issuing institution to pass certain account informa*tion, such as the card number and PIN number of a customer's debit card, to the acquirer **108**, thereby allowing the acquirer to process financial transactions that might not have been previously available to the acquirer (e.g., such as during an *online purchase*).

[0126] From the foregoing, it will be appreciated that specific embodiments of the invention have been described herein for purposes of illustration, but that various modifications may be made without deviating from the invention. For *example, those skilled in the art will further appreciate that* the depicted flow charts may be altered in a variety of ways. The order of the steps may be rearranged, steps may be performed in parallel, steps may be omitted, or other steps may be included. Accordingly, the invention is not limited *except as by the appended claims.*

I/We claim:

1. A method for managing payment instruments associated with customer accounts in a computing system controlled by an intermediary service, the computing system including a processor and a storage area, the method comprising:

maintaining customer accounts in the storage area, wherein each customer account includes an account identifier and information specifying one or more payment instruments associated with that customer account,

39

wherein each payment instrument is provided by an issuing institution different from the intermediary service;

maintaining information in the storage area that correlates payment instruments to issuing institutions that issued each payment instrument;

receiving a change request at the computing system of the intermediary service, wherein the change request includes an account identifier and specifies a change in status for a payment instrument associated with the account identifier;

determining the correlated issuing institution based on the specified payment instrument; and

based on the specified change in status, recording an indication that specifies whether the payment instrument is enabled or disabled,

wherein the recorded indication of whether the payment instrument is enabled or disabled is utilized to accept or reject an authorization request against the payment instrument.

2. The method of claim 1, wherein the indication of whether the payment instrument is enabled or disabled is recorded by transmitting a message to the issuing institution to enable or disable the payment instrument.

3. The method of claim 2, wherein the recorded indication is utilized by the issuing institution to accept or reject an authorization request against the payment instrument.

4. The method of claim 1, wherein the indication of whether the payment instrument is enabled or disabled is recorded at the intermediary service without transmitting a message to the issuing institution.

5. The method of claim 4, wherein the recorded indication is utilized by the intermediary service to accept or reject an authorization request against the payment instrument.

6. The method of claim 4, further comprising:

receiving an account status request from the issuing institution, wherein the account status request is generated in response to the issuing institution receiving an authorization request; and

sending a message including the recorded indication to the issuing institution.

7. The method of claim 1, wherein the change request further defines a change time for the specified change in status of the payment instrument, and wherein the change in status does not become effective until after the defined change time.

8. The method of claim 7, wherein the change request further defines an end time for the specified change in status of the payment instrument, and wherein the method further comprises, when the end time is reached, recording a modified indication that specifies whether the payment instrument is enabled or disabled.

9. The method of claim 8, wherein recording a modified indication comprises transmitting a message to the issuing institution to enable or disable the payment instrument.

10. The method of claim 1, further comprising verifying the authenticity of the change request in response to the change request, wherein the indication is recorded if the authenticity of the change request is verified.

11. The method of claim 10, wherein verifying the authenticity of the change request comprises:

transmitting a verification request message to a mobile device associated with the customer account; and

receiving a verification response message from the mobile device, wherein the verification response message includes a confirming response provided by a user of the mobile device.

12. The method of claim 11, further comprising transmitting a status change confirmation to the mobile device when the indication has been recorded.

13. The method of claim 1, wherein the change request is from a customer.

14. The method of claim 1, wherein the change request further specifies a change in status for a plurality of payment instruments.

15. The method of claim 1, further comprising:

determining that the authorization request will be rejected by the issuing institution;

transmitting a notification message to a mobile device associated with the customer account;

receiving a reactivation command from the mobile device; and

recording an updated indication that specifies that the payment instrument is enabled.

16. An intermediary service for managing payment instruments associated with customer accounts, the intermediary service comprising:

a processor;

a storage component configured to:

store customer accounts, wherein each customer account includes an account identifier and information specifying one or more payment instruments associated with that customer account, wherein each payment instrument is provided by an issuing institution different from the intermediary service, and

store information that correlates payment instruments to issuing institutions that issued each payment instrument;

a customer communication module configured to:

receive a change request, wherein the change request includes an account identifier and specifies a change in status for a payment instrument associated with the account identifier; and

an evaluation component configured to:

determine the correlated issuing institution based on the specified payment instrument; and

based on the specified change in status, record an indication that specifies whether the payment instrument is enabled or disabled,

wherein the recorded indication of whether the payment instrument is enabled or disabled is utilized to accept or reject an authorization request against the payment instrument.

17. The intermediary service of claim 16, wherein the indication of whether the payment instrument is enabled or disabled is recorded by transmitting a message to the issuing institution to enable or disable the payment instrument.

18. The intermediary service of claim 16, wherein the recorded indication is utilized by the issuing institution.

19. The intermediary service of claim 18, wherein the indication of whether the payment instrument is enabled or disabled is recorded without transmitting a message to the issuing institution.

20. The intermediary service of claim 19, wherein the recorded indication is utilized by the intermediary service.

21. The intermediary service of claim 16, wherein the change request further defines a change time for the specified

change in status of the payment instrument, and wherein the change in status does not become effective until after the defined change time.

22. The intermediary service of claim 21, wherein the change request further defines an end time for the specified change in status of the payment instrument, and wherein the request evaluation component is further configured to record, when the end time is reached, a modified indication that specifies whether the payment instrument is enabled or disabled.

23. The intermediary service of claim 22, wherein recording a modified indication comprises transmitting a message to the issuing institution to enable or disable the payment instrument.

24. The intermediary service of claim 16, wherein the evaluation component is further configured to verify the authenticity of the change request in response to the change request, wherein the indication is stored if the authenticity of the change request is verified.

25. The intermediary service of claim 24, wherein verifying the authenticity of the change request comprises:

transmitting a verification request message to a mobile device associated with the customer account; and

receiving a verification response message from the mobile device, wherein the verification response message includes a confirming response provided by a user of the mobile device.

26. The intermediary service of claim 25, wherein the evaluation component is further configured to transmit a status change confirmation to the mobile device when the indication has been recorded.

27. The intermediary service of claim 16, wherein the change request is from a customer.

28. The intermediary service of claim 16, wherein the change request further specifies a change in status for a plurality of payment instruments.

29. A computer-readable medium containing instructions for managing payment instruments associated with customer accounts in a computing system controlled by an intermediary service, the computing system including a processor and a storage area, by a method comprising:

maintaining customer accounts in the storage area, wherein each customer account includes an account identifier and information specifying one or more payment instruments associated with that customer account, wherein each payment instrument is provided by an issuing institution different from the intermediary service;

maintaining information in the storage area that correlates payment instruments to issuing institutions that issued each payment instrument;

receiving a change request at the computing system of the intermediary service, wherein the change request includes an account identifier and specifies a change in status for a payment instrument associated with the account identifier;

determining the correlated issuing institution based on the specified payment instrument; and

based on the specified change in status, recording an indication that specifies whether the payment instrument is enabled or disabled,

wherein the recorded indication of whether the payment instrument is enabled or disabled is utilized to accept or reject an authorization request against the payment instrument.

30. The computer-readable medium of claim 29, wherein the indication of whether the payment instrument is enabled or disabled is recorded by transmitting a message to the issuing institution to enable or disable the payment instrument.

31. The computer-readable medium of claim 29, wherein the recorded indication is utilized by the issuing institution.

32. The computer-readable medium of claim 29, wherein the indication of whether the payment instrument is enabled or disabled is recorded at the intermediary service without transmitting a message to the issuing institution.

33. The computer-readable medium of claim 32, wherein the recorded indication is utilized by the intermediary service.

34. The computer-readable medium of claim 29, wherein the change request further defines a change time for the specified change in status of the payment instrument, and wherein the change in status does not become effective until after the defined change time.

35. The computer-readable medium of claim 34, wherein the change request further defines an end time for the specified change in status of the payment instrument, and wherein the method further comprises, when the end time is reached, storing a modified indication that specifies whether the payment instrument is enabled or disabled.

36. The computer-readable medium of claim 35, wherein storing a modified indication comprises transmitting a message to the issuing institution to enable or disable the payment instrument.

37. The computer-readable medium of claim 29, further comprising verifying the authenticity of the change request in response to the change request, wherein the indication is stored if the authenticity of the change request is verified.

38. The computer-readable medium of claim 37, wherein verifying the authenticity of the change request comprises:

transmitting a verification request message to a mobile device associated with the customer account; and

receiving a verification response message from the mobile device, wherein the verification response message includes a confirming response provided by a user of the mobile device.

39. A method for controlling status of a payment instrument associated with a customer account, the method comprising:

providing information to enable an intermediary service to maintain a customer account in a storage area, wherein the customer account includes an account identifier and information specifying one or more payment instruments associated with the customer account, wherein each payment instrument is provided by an issuing institution different from the intermediary service, and wherein the storage area further includes information correlating payment instruments to issuing institutions that issued each payment instrument; and

submitting a change request to the intermediary service, wherein the change request includes an account identifier and specifies a change in status for a payment instrument associated with the account identifier;

wherein, in response to the change request, the intermediary service determines the correlated issuing institution based on the specified payment instrument and records

36

an indication that specifies whether the payment instrument is enabled or disabled based on the specified change in status, and

wherein the recorded indication of whether the payment instrument is enabled or disabled is utilized to accept or reject an authorization request against the payment instrument.

40. The method of claim 39, wherein the indication of whether the payment instrument is enabled or disabled is recorded by transmitting a message to the issuing institution to enable or disable the payment instrument.

41. The method of claim 40, wherein the recorded indication is utilized by the issuing institution to accept or reject an authorization request against the payment instrument.

42. The method of claim 39, wherein the indication of whether the payment instrument is enabled or disabled is recorded at the intermediary service without transmitting a message to the issuing institution.

43. The method of claim 42, wherein the recorded indication is utilized by the intermediary service to accept or reject an authorization request against the payment instrument.

44. The method of claim 39, wherein the change request further defines a change time for the specified change in status of the payment instrument, and wherein the change in status for the payment instrument does not become effective until after the defined change time.

45. The method of claim 44, wherein the change request further specifies an end time for the specified change in status of the payment instrument, and wherein the change in status for the payment instrument reverts back to an initial state after the end time.

46. The method of claim 44, further comprising receiving a notification message at a mobile device associated with the customer account, the notification message received in proximity to the change time and indicating a change of status at the change time.

47. The method of claim 46, wherein the notification message further comprises a cancellation option, the method further comprising:

sending a cancellation message from the mobile device, wherein the cancellation message indicates that the change of status should be canceled,

wherein the change in status for the payment instrument is not recorded when the intermediary service receives the cancellation message.

48. The method of claim 46, wherein the notification message further comprises a modify option, the method further comprising:

sending a modification message from the mobile device, wherein the modification message indicates that the change of status should be recorded at a second change time,

wherein the change in status for the payment instrument is recorded at the second change time in response to the modification message.

49. The method of claim 39, wherein the change request is submitted via a mobile device associated with the customer account.

50. The method of claim 39, further comprising:

receiving a verification request message at a mobile device associated with the customer account, the verification request message seeking a confirmation of the change request; and

sending a verification response message from the mobile device, wherein the verification response message includes a confirmation of the change request provided by a user of the mobile device,

wherein the indication is recorded in response to the intermediary service receiving the verification response message.

* * * * *

37

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
NIT : 800.176.089-2
- / -

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 110080

Bogotá D.C., Octubre 16 de 2014 - 15:52:38

RECIBIDO DE : MUÑOZ ABOGADOS COMPAÑIA LIMITADA IURIS MARK LTDA NI 830.090.578

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	613562456	09/10/2014	335.000.00

*** Conceptos Pagados ***

CANT	RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
1	50005-01-04 PRESENTACION DE OBSERVACIONES A SOLICITUDES	12 OPOSICION POR CADA CLASE-MARCAS Y LEMAS COMERCIALES	335.000.00	335.000.00
				$335.000.00

SON: **TRESCIENTOS TREINTA Y CINCO MIL PESOS MONEDA CORRIENTE*

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
No. 14-148885- -00002-0000
Fecha: 2014-10-16 16:47:41 Dep: 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
Act. 400 OPOSIOBSERVTER Folios: 38