TÉRMINOS Y CONDICIONES DE USO DEL SERVICIO PORTAL TRANSACCIONAL/BANCA MÓVIL

Mediante el presente documento se regula el uso y manejo del servicio de PORTAL TRANSACCIONAL/BANCA MÓVIL que LA ENTIDAD pone a disposición del cliente, en adelante el ASOCIADO/CLIENTE:

1. **DEFINICIONES:**

1.1. **Banca móvil:** es el canal electrónico transaccional a través del cual todo ASOCIADO/CLIENTE que esté registrado en el PORTAL TRANSACCIONAL/BANCA MÓVIL de LA ENTIDAD, podrá realizar transacciones financieras vía celular, de una forma fácil, segura y oportuna.

1.2. **Interbancarias enviadas:** son las operaciones que realiza el ASOCIADO/CLIENTE debitando del producto que tenga en LA ENTIDAD, con destino a una cuenta bancaria propia o de otro destinatario.

1.3. **Interbancarias recibidas:** son las operaciones que realiza el ASOCIADO/CLIENTE debitando del producto que tenga en un Establecimiento de Crédito, con destino a LA ENTIDAD.

1.4. **Mensajes SMS (Short Messaginng System):** servicio disponible en los teléfonos celulares que permite el envío de mensajes cortos (también conocidos como mensajes de texto) entre teléfonos móviles, y otros dispositivos de mano.

1.5. **Portal transaccional/Banca móvil:** es un canal ofrecido por LA ENTIDAD para facilitar a sus ASOCIADOS/CLIENTES el acceso a los productos y servicios brindados a través de medios electrónicos no presenciales.

1.6. **PSE:** es un sistema centralizado y estandarizado, desarrollado por ACH COLOMBIA que permite a la entidad brindar a sus ASOCIADOS/CLIENTES la posibilidad de efectuar pagos a través de la página de internet, debitando los recursos de los productos que el ASOCIADO/CLIENTE tiene en LA ENTIDAD.

1.7. **Teléfono Celular:** dispositivo inalámbrico que permite tener acceso a la red de telefonía celular, con capacidad de procesamiento y conexión permanente o intermitente a una red de internet, a través del cual se accede al servicio de BANCA MÓVIL.

2. **OBJETO:** establecer las condiciones y reglas de uso aplicables al canal de PORTAL TRANSACCIONAL/BANCA MÓVIL para que LA ENTIDAD y sus ASOCIADOS/CLIENTES tengan claridad en el manejo del mismo y el conocimiento necesario para atender requerimientos que surjan durante la vigencia del vínculo comercial y utilización del canal.

3. CONDICIONES DEL SERVICIO.

3.1. El servicio ofrecido por parte de LA ENTIDAD a través del PORTAL TRANSACCIONAL/BANCA MÓVIL es exclusivo para las personas naturales que se encuentran vinculadas a LA ENTIDAD con cualquier producto ofrecido por LA ENTIDAD.

3.2. LA ENTIDAD procurará que el servicio esté disponible para el ASOCIADO/CLIENTE las veinticuatro (24) horas, los 365 días al año, sin perjuicio de las limitaciones y restricciones de operaciones y/o transacciones específicas establecidas e informadas por LA ENTIDAD al ASOCIADO/CLIENTE. No obstante lo anterior, LA ENTIDAD puede suspender, restringir o modificar su funcionamiento, temporal o definitivamente a un determinado horario o para una clase de operaciones y/o transacciones específicas.

3.3. Para las transferencias interbancarias, el envío por parte de LA ENTIDAD al Banco que recibe la transferencia de fondos será el mismo día, siempre y cuando esta se haya realizado en el horario de 8:00 AM a 2:00 PM en días hábiles; las operaciones y/o transacciones que se realicen entre las 2:01 PM a 7:59 AM en días hábiles, sábados domingos y festivos a cualquier hora, serán enviados por LA ENTIDAD en el ciclo del siguiente día hábil. La aplicación será de acuerdo a las políticas del Banco que recibe la transferencia de fondos.

3.4. Para poder acceder al servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL, el ASOCIADO/CLIENTE deberá: i) Ser titular por lo menos de un producto en LA ENTIDAD. ii) Registrarse en este canal no presencial y disponer de un usuario autorizado y una clave principal, las cuales deben estar activos en el PORTAL TRANSACCIONAL/BANCA MÓVIL iii) Registrar el número del celular y correo electrónico en LA ENTIDAD. iv) Disponer de un teléfono celular que opere con sistema operativo Android o IOS. v) Contar con un plan de datos con un operador celular o conexión a Internet WiFi. vi) Autorizar en LA ENTIDAD, el envío de SMS (mensajes de texto) y/o correos electrónicos.

3.5. Este canal electrónico no presencial permitirá al ASOCIADO/CLIENTE realizar las siguientes operaciones: transferencias (Intracooperativas, Intercooperativas e Interbancarias), pago de obligaciones, los pagos disponibles en PSE y las demás que se encuentren disponibles en el PORTAL TRANSACCIONAL/BANCA MÓVIL, y aquellas que se implementen en el futuro.

3.6. El ASOCIADO/CLIENTE podrá utilizar los servicios electrónicos ofrecidos por LA ENTIDAD durante el término de vigencia de los productos de los cuales es titular en LA ENTIDAD.

3.7. LA ENTIDAD podrá establecer límites máximos y mínimos para las operaciones y transacciones a través del servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL, los cuales, de establecerse, serán informados en las carteleras de las oficinas de LA ENTIDAD o a través de cualquier otro medio idóneo. Las operaciones y/o transacciones del

ASOCIADO/CLIENTE se atenderán siempre y cuando el saldo de lo(s) respectivo(s) productos(s) lo permita.

3.8. LA ENTIDAD procesará la información y las operaciones en el momento en que el ASOCIADO/CLIENTE active el servicio mediante la respectiva clave y/o seguridades establecidas o que llegaren a habilitarse, siempre y cuando fueren legales o convencionalmente posibles, no obstante lo anterior, las operaciones y/o transacciones que realice con la información suministrada durante el día estarán sometidas a verificación por parte de LA ENTIDAD, autorizando el ASOCIADO/CLIENTE desde ahora los ajustes, débitos o créditos, que éste efectúe en las respectivas cuentas o créditos en razón de dicha verificación, que en todo caso será justificada.

3.9. El producto provee privacidad de la información del ASOCIADO/CLIENTE y de los datos relativos a la transaccionalidad e integridad en los mensajes intercambiados y mecanismos que permitan que una vez realizada una transacción, quede constancia de ello.

3.10. La clave de acceso y el usuario identificará al ASOCIADO/CLIENTE en sus relaciones con LA ENTIDAD vía internet, y estarán bajo su control exclusivo. Adicionalmente, el ASOCIADO/CLIENTE asumirá todos los riesgos, costos y pérdidas incurridas que tengan origen o que estén relacionados con el uso no autorizado de los servicios y de la utilización y custodia de sus claves las cuales son personales e intransferibles. Cualquier operación realizada por el ASOCIADO/CLIENTE con la utilización de su clave será entendida como emanada válida, legítima y auténticamente por éste, sin que LA ENTIDAD tenga la obligación de realizar o tomar resguardo adicional en tal sentido. El ASOCIADO/CLIENTE no podrá oponer defensa alguna basada en defecto de acreditación, asumiendo el ASOCIADO/CLIENTE toda la consecuencia jurídica del uso del sistema en su nombre.

3.11. LA ENTIDAD se reserva el derecho a limitar, suspender y/o cancelar el servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL a los ASOCIADOS/CLIENTES que incumpla(n) o contraríe(n) lo dispuesto en los presentes términos y condiciones, o que utilicen el servicio con la finalidad de cometer actos fraudulentos, delictivos , o llegare a ser (i) vinculado por parte de las autoridades competentes a cualquier tipo de investigación por delitos de narcotráfico, terrorismo, secuestro, lavado de activos, financiación del terrorismo y administración de recursos relacionados con actividades terroristas u otros delitos relacionados con el lavado de activos y financiación del terrorismo, (ii) incluido en listas para el control de lavado de activos y financiación del terrorismo administradas por cualquier autoridad nacional o extranjera, tales como la lista de la Oficina de Control de Activos en el Exterior — OFAC emitida por la Oficina del Tesoro de los Estados Unidos de Norte América, la lista de la Organización de las Naciones Unidas y otras listas públicas relacionadas con el tema del lavado de activos y financiación del terrorismo, o (iii) condenado por parte de las autoridades competentes en cualquier tipo de proceso judicial relacionado con la comisión de los anteriores delitos, sin que ellos genere indemnización alguna.

3.12. El ASOCIADO/CLIENTE debe verificar, antes de realizar sus operaciones y/o transacciones que tenga saldo disponible o que la información sea correcta, toda vez que estas quedan registradas en los archivos del servicio y luego de ser confirmadas no pueden ser reversadas, modificadas o canceladas, siempre que se compruebe un acceso exitoso.

3.13. LA ENTIDAD atenderá y gestionará los reclamos formulados por los ASOCIADOS/CLIENTES relacionados con las operaciones y/o transacciones realizadas a través del servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL.

3.14. El ASOCIADO/CLIENTE conviene que LA ENTIDAD podrá en cualquier tiempo modificar las condiciones, modalidades u operaciones de estos sistemas, con el objeto de obtener un mejor aprovechamiento de los servicios del PORTAL TRANSACCIONAL/BANCA MÓVIL, situaciones que serán notificadas previamente a través de los medios que el ASOCIADO/CLIENTE tenga habilitados en la ENTIDAD.

3.15. El ASOCIADO/CLIENTE autoriza a LA ENTIDAD para originar y/o recibir transacciones débito y/o transacciones crédito, según el caso, a través de ACH COLOMBIA.

3.16. El ASOCIADO/CLIENTE declara y garantiza que ha obtenido de los Usuarios Receptores a quienes enviará transacciones débito, las correspondientes autorizaciones para que estos acepten y apliquen las transacciones débito enviadas por El ASOCIADO/CLIENTE.

4. OBLIGACIONES DEL ASOCIADO/CLIENTE.

4.1. El ASOCIADO/CLIENTE debe velar por el uso y resguardo de sus claves personales y procurar realizar sus operaciones y/o transacciones desde equipos seguros. El ASOCIADO/CLIENTE es responsable de tomar las medidas de seguridad necesarias para precaver virus y/o otros actores nocivos que circulan por Internet en los equipos que el ASOCIADO/CLIENTE utilice.

4.2. El ASOCIADO/CLIENTE verificará la información antes de realizar sus operaciones y/o transacciones para evitar inconsistencias toda vez que los registros electrónicos que se generen bajo la clave, firma digital, firma electrónica y/o seguridades adicionales, serán prueba de sus operaciones y/o transacciones. Es responsabilidad del ASOCIADO/CLIENTE verificar la exactitud de la información que suministre para hacer uso de los servicios del PORTAL TRANSACCIONAL/BANCA MÓVIL, tales como números de cuenta, números de recibos, valor de los recibos, entre otros.

4.3. Inscribir y actualizar en LA ENTIDAD a través de los mecanismos establecidos por ella, el correo electrónico y el número del celular desde el cual se podrán generar mensajes de texto para realizar las operaciones y/o transacciones, recibir los servicios y suministrar la información que LA ENTIDAD le solicite.

4.4. Cambiar su clave cada vez que el sistema lo alerte. De igual forma la podrá modificar en cualquier momento.

4.5. Seguir las recomendaciones formuladas por LA ENTIDAD en cuanto a forma de operar y seguridades del servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL.

4.6. Actualizar sus datos en la entidad para que pueda recibir las comunicaciones oportunamente y utilizar el canal y sus productos sin interrupciones.

4.7. En caso de pérdida o hurto del celular notificar inmediatamente a LA ENTIDAD, por la vía más rápida para que LA ENTIDAD tome las medidas convenientes.

5. SUSPENSIÓN DEL SERVICIO: LA ENTIDAD podrá en cualquier momento interrumpir o suspender el servicio por razones técnicas, de seguridad, por los problemas que puedan presentarse por cortes en los servicios de teléfonos celulares, energía, por fuerza mayor, caso fortuito o hecho de un tercero, entre otros y velará porque estas suspensiones sean notificadas al ASOCIADO/CLIENTE inclusive después de ocurridas, conforme con lo establecido en las normas de información a consumidores financieros.

6. RECOMENDACIONES DE SEGURIDAD

6.1. PORTAL TRANSACCIONAL/BANCA MÓVIL

- ✓ La Clave Principal y Segunda Clave es personal e intransferible, no se puede compartir con nadie. Dar a conocer las claves generará riesgos de fraudes.
- ✓ No escriba la clave en ningún lado, memorícela.
- ✓ LA ENTIDAD nunca solicitará el cambio de la clave principal a través de correo electrónico o mensajes de texto.
- ✓ Cuando defina “las preguntas de seguridad”, evite ingresar respuestas obvias o que sean conocidas por terceras personas, utilice contraseñas fáciles de recordar para usted, no utilice fechas de nacimiento, número de documento de identidad, dirección o teléfonos, memorícelas y no las escriba en ningún lugar.
- ✓ Realice cambios de clave de manera preventiva, por lo menos una vez por mes.
- ✓ El uso de su usuario y contraseña de acceso al sistema es responsabilidad de usted, no permita que otra persona las utilice.
- ✓ Realice sus operaciones y/o transacciones únicamente desde equipos de uso personal, en su casa u oficina, evite el uso de equipos ubicados en sitios públicos que no sean de absoluta confianza como un café internet, salas universitarias o lugares donde extraños puedan tener acceso a su información confidencial.
- ✓ Nunca preste su cuenta para recibir fondos cuyo origen usted desconoce, delincuentes utilizan este método para la transferencia de dinero de procedencia ilícita.

- ✓ Nunca ingrese a través de enlaces en correos electrónicos falsos (phishing), que puedan llevarle a sitios fraudulentos. Recuerde que la ENTIDAD no solicita información confidencial por este medio.
- ✓ Instale y mantenga actualizado su computador con herramientas de seguridad informática (antivirus, antispyware, firewall personal y actualizaciones del sistema operativo), lo cual le protege contra espionaje y robo de información.
- ✓ Mantenga los navegadores actualizados a su última versión.
- ✓ Si utiliza un computador portátil, le recomendamos no acceder al PORTAL TRANSACCIONAL/BANCA MÓVIL desde una conexión inalámbrica (WiFi) pública, por ejemplo en aeropuertos o parques.
- ✓ Usted debe tener total confidencialidad con la información de los usuarios y claves de acceso al PORTAL TRANSACCIONAL/BANCA MÓVIL.
- ✓ Una vez termine sus operaciones y/o transacciones en el PORTAL TRANSACCIONAL/BANCA MÓVIL debe asegurarse de realizar el cierre de sesión de forma segura.
- ✓ Si le llega un reporte de una transacción que usted no ha realizado debe proceder de inmediato a bloquear el canal del PORTAL TRANSACCIONAL/BANCA MÓVIL, comunicándose con LA ENTIDAD.
- ✓ Cuando ingrese a la página web de la ENTIDAD verifique siempre que la imagen del candado en la parte superior de su navegador, aparezca y se encuentre cerrado.
- ✓ Cuando realice compras por Internet, cerciórese que sean páginas seguras (verificando que esté presente el candado de seguridad en la parte inferior, o muestre en la dirección el prefijo https) de lo contrario no estará segura la confidencialidad de sus datos personales y financieros.
- ✓ Evite descargar e instalar programas de fuentes desconocidas, estos pueden contener programas escondidos o virus que pueden comprometer su información.
- ✓ Mantenga actualizado su computador con herramientas de seguridad como antivirus, antispyware, firewall personal, y actualizaciones del sistema operativo, con el fin de protegerse de programas maliciosos que sustraigan su información.
- ✓ Evite proporcionar datos personales a través del perfil de las redes sociales (Facebook, Twitter, Pinterest, etc.)
- ✓ Evite diligenciar formularios en sitios web para suscribirse a boletines en línea o participar en rifas.
- ✓ Evite diligenciar formularios físicos donde le solicitan actualizar datos a cambio de algún beneficio.

6.2. BANCA MOVIL

- ✓ Mantenga el teclado de su teléfono celular bloqueado, No lo deje desatendido, no lo preste a desconocidos.
- ✓ Utilice una clave de acceso al celular que no sea obvia y no la comparta.
- ✓ Recuerde cambiar regularmente la contraseña de Banca Móvil.

- ✓ No almacene nunca las contraseñas de acceso al móvil o a los servicios financieros en los listines del móvil o en archivos dentro del mismo. En caso de que así lo requiera haga uso de programas para cifrado de datos.
- ✓ No descuide su celular. En caso de pérdida o robo de su teléfono celular, comuníquese inmediatamente con su operador e inhabilite su número, también informe a LA ENTIDAD para el bloqueo del canal.
- ✓ Si acostumbra instalar o bajar aplicaciones (programas) en su equipo móvil hágalo solo de sitios conocidos que garanticen la no presencia de programas maliciosos (malware, spyware, virus), valide las condiciones de uso antes de aceptar la instalación.
- ✓ No navegue en sitios desconocidos con su móvil. Podría tener ataques similares a los que se tiene en el PC.
- ✓ Si su equipo móvil requiere de mantenimiento o actualizaciones nunca entregue las claves de acceso al personal de mantenimiento. Además valide que no le hayan instalado programas o aplicaciones diferentes a las que usted normalmente utiliza.
- ✓ No habilite por defecto los puertos bluetooth. Solo hágalo para conectarse a los dispositivos que utiliza con el móvil. Configure la autenticación para dichos puertos evitando que un desconocido se pueda conectar a su móvil sin su conocimiento.
- ✓ Si hace uso de conexiones WIFI en su móvil utilice protocolos seguros (WPA, WPA2) y no se conecte a redes desconocidas. No mantenga activa la conexión WIFI.
- ✓ Si su móvil tiene opciones de seguridad adicionales (caso de blackberry, Iphone, equipos de alta gama y algunos de media) haga uso de ellas y conozca con detalle las funcionalidades que prestan.
- ✓ Si acostumbra hacer backup del software de su móvil y de los datos guardados en él, hágalo en una estación (PC) conocida y asegúrese de que sólo usted tenga acceso a dicha información. Utilice programas para protección de su móvil, si éste cuenta con los aplicativos para ello. Hoy existen para determinados equipos soluciones de antivirus y similares.

6.3. MODALIDADES DE FRAUDE

Ingeniería Social: es el conjunto de técnicas que los delincuentes usan para manipular a las personas a través de engaño telefónico, presencial o por internet, buscando apropiarse de su información personal y financiera, como sus números de identificación y las claves de sus productos bancarias. En general el fraude se comete a través de alguna de las siguientes modalidades, entre otras:

- ✓ **Phishing:** envío de correos electrónicos que aparentan provenir de fuentes fiables (por ejemplo, entidades bancarias), para obtener datos confidenciales del usuario, que posteriormente se utilizan para la realizar fraudes.
- ✓ **Trashing:** recolectar información de documentos eliminados, comúnmente con la finalidad de obtener datos que sirvan como información para cometer fraudes.

- ✓ **Pharming:** explotación de una vulnerabilidad en el software de los equipos de los usuarios, que permite a un atacante redirigir una página web a otra distinta para el robo de información.
- ✓ **Vishing:** práctica fraudulenta que consiste en el uso del Protocolo Voz y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad.
- ✓ **Smishing:** envíos selectivos de mensajes SMS dirigidos a usuarios de telefonía móvil con el fin de que visiten una página web fraudulenta. Mediante reclamos atractivos con alertas urgentes, ofertas interesantes o suculentos premios, tratan de engañar al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.
- ✓ **Whaling:** técnicas de phishing dirigidas contra objetivos de alta importancia dentro de una organización (altos directivos de empresa, políticos, etc.) o simplemente de gran transcendencia social.

7. COSTOS: Las tarifas, costos y tasas que puedan aplicarse al uso de este canal serán publicadas en la página web de LA ENTIDAD o en sus oficinas y serán comunicadas al ASOCIADO/CLIENTE por los medios autorizados por el para que 45 días calendario previos a su entrada en vigencia el ASOCIADO/CLIENTE pueda conocerlas y definir si desea continuar con el uso del canal, lo cual puede comunicarlo por los medios habilitados por la entidad para la recepción de PQRSF**.**

8. TERMINACIÓN DE LA PRESTACIÓN DEL SERVICIO: El servicio del PORTAL TRANSACCIONAL/BANCA MÓVIL qué trata los términos y condiciones del presente documento, se podrá dar por terminado unilateralmente por parte de LA ENTIDAD, en los siguientes eventos:

8.1. Ante el incumplimiento por parte del ASOCIADO/CLIENTE de cualquiera de las obligaciones contenidas en estos términos y condiciones, o de las que por Ley se entiendan incorporadas al mismo.

8.2. Cuando se cancelen los productos de los cuales sea titular el ASOCIADO/CLIENTE.

No obstante lo anterior, cada una de las partes podrá darlo por terminado de forma unilateral en cualquier momento, asumiendo los costos que se adeuden, si a ello hubiere lugar.

9. VIGENCIA Y MODIFICACIÓN: Los actuales términos y condiciones son de vigencia indefinida y podrán ser modificados, adicionados, suprimidos o cancelados por LA ENTIDAD en cualquier momento, para lo cual LA ENTIDAD informará al ASOCIADO/CLIENTE y usuarios oportunamente,, por el canal que el ASOCIADO/CLIENTE tenga habilitado y por los medios que LA ENTIDAD considere apropiados.