Grupo de Acción Financiera de Sudamérica
Grupo de Açao Financeira da América do Sul

# INFORME SOBRE NUEVOS MÉTODOS DE PAGO: TARJETAS PREPAGAS, PAGOS POR TELEFONÍA MÓVIL Y PAGOS POR INTERNET

***- JUNIO 2013 -***

**Proyecto GAFISUD-Unión Europea**

*El presente documento ha sido producido con la asistencia financiera de la Unión Europea. El contenido del documento es responsabilidad de GAFISUD y de ninguna manera podrá interpretarse que el mismo refleja la posición de la Unión Europea.*

## TABLA DE CONTENIDOS

# CAPÍTULO 1: INTRODUCCIÓN

## *Antecedentes*

En el año 2009 la Unión Europea comienza a desarrollar el programa denominado **"Apoyo a la lucha contra el crimen organizado en la ruta de la cocaína".**

Como uno de los componentes de esa acción global, en diciembre de 2009 se suscribe un acuerdo entre la Unión Europea y GAFISUD para desarrollar el proyecto **"Apoyo al combate contra el lavado de activos en los países de América Latina y el Caribe**".

El objetivo central del proyecto en su primera fase era fortalecer el sistema preventivo en el sector financiero no bancario, y al realizarse el análisis de las amenazas a enfrentar, se evidenció la vulnerabilidad existente frente a la difusión en los países miembros de GAFISUD de métodos de pago no tradicionales que requerían una atención prioritaria.

Fue en ese contexto, que el equipo encargado del Proyecto encaró la elaboración y difusión del presente informe.

## *Objetivos del Informe*

Durante la última década los métodos de pago tradicionales se han ido encontrando con alternativas emergentes como las tarjetas prepagas, el pago móvil o los pagos por Internet. A medida que estos nuevos competidores se ponían en funcionamiento, comenzaron a dejar traslucir que no venían totalmente solos, sino que los acompañaba una amplia gama de amenazas relacionadas con el lavado de activo y la financiación del terrorismo (LA/FT).

El Grupo de Acción Financiera (GAFI, por sus siglas en francés) mostró su interés por estos nuevos métodos de pago (NMPs) desde su primera ola de difusión, ya que experimentaron un notable aumento tanto en su número de usuarios como en la cantidad de fondos empleados. Como fruto de su interés, GAFI presentó en 2006 un informe con los peligros latentes que estos métodos acarreaban. Incidiendo en el informe de 2006, GAFI presentó en 2010 un nuevo informe a modo de actualización donde se comparaban y contrastaban con más evidencias los riesgos descritos en 2006 junto con los riesgos actuales basados en casos y tipologías. Desde la publicación de su último informe, GAFI ha continuado investigando sobre el tema y actualmente se encuentra en el proceso de presentar una guía sobre el enfoque basado en el riesgo de los NMPs.

En línea con el trabajo de GAFI, GAFISUD ha querido comprender mediante el presente informe la situación en la región, y especialmente el grado de conocimiento por parte de los Estados miembros de estas nuevas alternativas de pago. GAFISUD ha notado una carencia generalizada de información al respecto, y ésta está directamente relacionada con el aún poco desarrollo mercado de los NMPs. GAFISUD entiende, en concordancia con los estudios disponibles y con la idiosincrasia de la región, que los NMPs en Latinoamérica presentan las mejores condiciones para experimentar un desarrollo profundo a lo largo de los próximos años, y que por lo tanto hay que incidir en su regulación para evitar el abuso por parte de los criminales en operaciones de LA/FT.

El objetivo de GAFISUD es entender en su totalidad las características, funcionamiento, modalidades y riesgos de estos métodos de pago, así como identificar aquellos elementos que puedan funcionar como mitigadores de esas amenazas. Se pretende mantener un enfoque que preserve la viabilidad de los productos y servicios promoviendo por un lado la inclusión financiera, y por otro, el cumplimiento de requisitos razonables de control, supervisión y seguridad. En una etapa posterior, GAFISUD podrá proporcionar toda la asistencia que los países miembros necesiten al respecto para revisar su situación nacional y traerla a los máximos niveles de efectividad cumpliendo con los principales estándares internacionales.

### *Estructura del Presente Informe*

El presente informe está basado en las publicaciones del GAFI de 2006 y 2010, así como en sus líneas de trabajo actuales. GAFISUD ha procurado reunir toda la información disponible para tener una visión holística de todos los aspectos que caracterizan estos tres nuevos métodos de pago y producir un informe que facilite su entendimiento a los Estados miembros asentando las bases de los posibles pasos a tener en cuenta, y que son de común interés para la región.

Este informe se divide en cinco módulos:

- Los Capítulos 1 y 2 ofrecen una visión detallada de cada unos de los métodos de pago, su evolución, características y funcionamiento;

- Los Capítulos 3, 4 y 5 se centran en la identificación de riesgos y en las formas de mitigarlos acorde con los estándares internacionales. Este módulo incluye también una selección de casos de explotación de NMPs por criminales para operaciones de LA. Finalmente, en el Capítulo 5 se hace hincapié en la compatibilidad del cumplimiento de las recomendaciones del GAFI y la inclusión financiera.

- El Capítulo 6 concluye con una visión general de la situación del subsector de pagos en la región latinoamericana.

- El Capítulo 7 describe tres casos de productos particulares; en los dos primeros existe normativa que pretende mitigar los riesgos detectados, mientras que en el tercer caso se describe un esquema no regulado de moneda virtual multiuso.

- El Capítulo 8 recoge brevemente las principales conclusiones del informe.

> Para indicarlo de forma sucinta y en término actuales, el destino del dinero es convertirse en digital. Esta conclusión general emerge del examen de los largos registros históricos del dinero y su probable relación con los futuros cambios socioeconómicos. Históricamente, durante milenios, el dinero ha estado en la senda de una mayor abstracción, o pura representación desasociada de una materialización física precisa.
>
> Organización para la Cooperación y Desarrollo Económicos
> The Future of Money[1]

## *Situación Actual*

El desarrollo tecnológico continúa su carrera avanzando a ritmos desenfrenados y aplicándose en todos los sectores existentes en pos de facilitar la vida de sus usuarios. En el sector que nos interesa—el sector de pagos—el empleo de nuevas tecnologías ha propiciado la aparición de nuevos métodos que, gracias a las ventajas y beneficios que ofrecen, se han expandido vertiginosamente, gozando de amplia aceptación y satisfaciendo las necesidades de un mundo cada vez más digitalizado que requiere nuevas formas de pago para operaciones más convenientes, más seguras, viables desde cualquier lugar y accesibles a la gran mayoría de las personas. Esta adaptación tecnológica está ocurriendo a ritmos tan veloces que dificulta la posibilidad de que las regulaciones anti-lavado de activos y contra el financiamiento del terrorismo (ALA/CFT) se ajusten a la nueva realidad sin quedar nuevamente desfasadas.

En el sector de pagos, los nuevos métodos emergentes, presentan un futuro prometedor, especialmente al estar dirigidos a un nicho de millones de personas aún por explotar que buscan poder utilizar medios de pago en los que no se vean involucradas instituciones financieras bancarias, o que simplemente ofrezcan más practicidad, seguridad y confidencialidad que los métodos tradicionales.

El éxito de estos métodos coincide con la ampliación de sus propias funcionalidades; ahora permiten, entre otras muchas operaciones, hacer transferencias nacionales e internacionales, efectuar y recibir pagos desde cualquier lugar, e incluso la posibilidad de retirar efectivo desde cajeros automáticos sin tener que disponer de una cuenta bancaria, de una tarjeta de crédito y/o débito, o sin tener que identificarse.

> En 2009, más de un millón de pakistaníes se vieron desplazados de sus hogares debido a conflictos en el país. El Gobierno de Pakistán, en su afán de proporcionar asistencia económica de forma rápida a estas personas, cooperó con un banco para distribuir tarjetas prepagas. Mediante esta iniciativa y con la instalación de terminales de puntos de venta donde las personas podían adquirir productos de necesidad básica, el Gobierno de Pakistán asistió aproximadamente a 300.000 personas.[2]

[1] OECD Report, *The Future of Money*, París, 2002, p.7. Traducido del Inglés, http://www.oecd.org/sti/futures/35391062.pdf

[2] FATF Report, *Money Laundering Using New Payment Methods*, Octubre 2010, París, p.12-13. http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

A pesar de que las oportunidades y ventajas que brindan estos métodos son incalculables, cabe apuntar que no siempre quedan eximidos de riesgos de LA/FT. En ocasiones, estos métodos pueden sobrepasar los márgenes de la legalidad y jugar a favor del mundo del crimen, particularmente debido a las lagunas regulatorias que experimentan al quedar fuera de las normativas por las que deben regirse los servicios financieros bancarios tradicionales. Estas fallas del sistema son fuertemente codiciadas por criminales tan variados como terroristas, traficantes de armas, bandas criminales o narcotraficantes que siempre se han mantenido a la última en metodología y tecnología para estar un paso por delante de las autoridades de control y poder encontrar las grietas de un sistema que explotar.

Los NMPs abarcan una amplia gama de productos que van desde meras extensiones del alcance de los sistemas de pago tradicionales a métodos totalmente nuevos. Acorde con la línea de trabajo del GAFI al respecto, este informe se centra en los siguientes NMPs: **Tarjetas Prepagas, Servicios de Pago Móvil y Servicios de Pago por Internet**.

# CAPÍTULO 2: NUEVOS MÉTODOS DE PAGOS

Esta sección se centra en tratar cada uno de los tres métodos de pago por separado con el objetivo de tener un entendimiento exhaustivo de su evolución, características, modalidades y funcionamiento.

## *2.1 Tarjetas Prepagas*

Las tarjetas prepagas aparecieron a finales de la década de los noventa como una alternativa a las tarjetas de crédito y/o débito. Esta nueva modalidad de tarjeta mantenía las mismas prestaciones y funcionalidades que las tradicionales pero sin necesitar una cuenta bancaria o una verificación de solvencia crediticia.

Las tarjetas prepagas pueden clasificarse en dos categorías principales: de ciclo abierto y de ciclo cerrado.[3] En lo que concierne al LA/FT, son las tarjetas de ciclo abierto las que más nos interesan puesto que su gran funcionalidad comporta mayores riesgos.

La modalidad de ciclo cerrado abarca a las generalmente conocidas como "tarjetas regalo"; la mayor parte de estas tarjetas suele tener un menor alcance de uso, reduciéndose éste a un comercio. Las tarjetas regalo son anónimas, no están asociadas a una cuenta bancaria, y no permiten extraer efectivo ni realizar transacciones. Sin embargo, es preciso apuntar, que no por el hecho de tener un uso limitado están exentas del riesgo de ser utilizadas ilícitamente para operaciones de LA/FT.

Un caso ilustrativo se dio en Estados Unidos en 2007. Criminales utilizaron tarjetas de crédito robadas para comprar tarjetas regalo que usaban para comprar mercancía que posteriormente era devuelta a las tiendas a cambio de nuevas tarjetas regalo; en ocasiones también revendían la mercancía para conseguir dinero en efectivo. Las nuevas tarjetas regalo ya no estaban relacionadas con las tarjetas de crédito robadas con las que se compraron las primeras tarjetas, por lo tanto quedaban impunes a efectos de cualquier investigación.[4]

**Tarjetas regalo**

[3] Se pueden también nombrar dos subdivisiones, las tarjetas semiabiertas que tienen las mismas características que las abiertas pero no pueden retirar efectivo desde cajeros; y las semicerradas permiten pagar productos y servicios ya no sólo en un comercio sino en un grupo determinado de ellos.
[4] FATF Report, *Money Laundering Using New Payment Methods*, Octubre 2010, París, p.14. http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

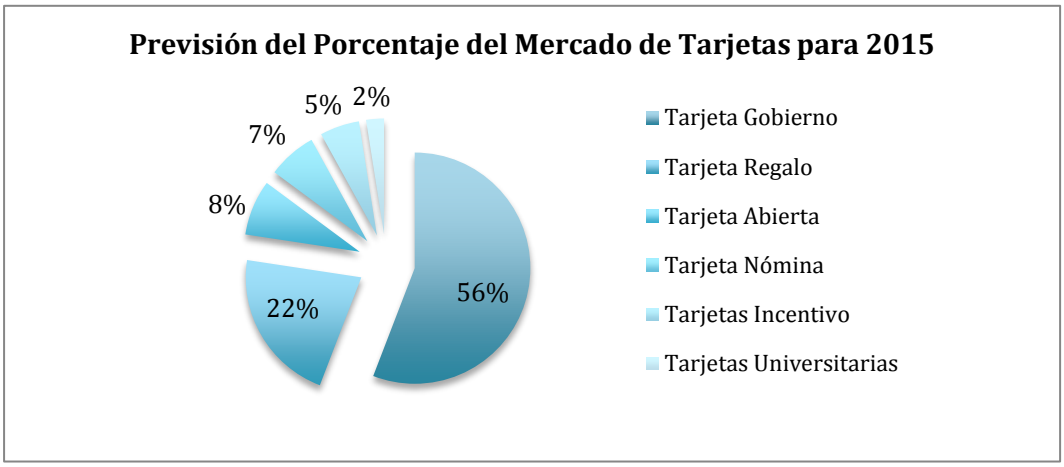
Al igual que las tarjetas regalo, las tarjetas de ciclo abierto son anónimas y no necesitan estar asociadas a ninguna cuenta bancaria. Se diferencian principalmente de las tarjetas regalo porque tienen mayor alcance de uso, tanto comercial como geográfico y operacional. Además, según la idiosincrasia del programa de tarjetas, éstas pueden ser recargables o de un solo uso. En definitiva, debido a sus funcionalidades, las tarjetas prepagas se convierten en una alternativa a muchos productos y servicios bancario tradicionales; obsérvese que muchas ofrecen características similares a las cuentas bancarias (se puede efectuar y recibir pagos de terceros, retirar dinero en efectivo de las redes globales de cajeros automáticos, enviar o recibir remesas, etc.).


**Tarjetas abiertas**

En su conjunto, las tarjetas prepagas abarcan un nicho de mercado más amplio que el de las tarjetas o sistemas de pagos tradicionales porque pueden incluir tanto a personas bancarizadas como a no bancarizadas. Entre las claves de su éxito se destaca su idoneidad para controlar exhaustivamente el gasto. Se ha notado que en muchos de los países que han sufrido o sufren crisis económicas el uso de estas tarjetas ha experimentado un crecimiento sostenido.

Actualmente, la demanda de tarjetas prepagas está aumentando de manera exponencial. Estimaciones de analistas[5] afirman que para el año 2015 este mercado alcanzará los 762 mil millones de dólares. Las tarjetas que destinan los gobiernos para beneficios sociales representan el segmento más grande con un potencial de 425 mil millones de dólares, junto a las tarjetas regalo con 164 mil millones. Les siguen las tarjetas abiertas comunes con 59 mil millones, las tarjetas destinadas a pagar nómina de trabajadores con 52 mil millones, las tarjetas de incentivos ofrecida por el sector privado a sus trabajadores o clientes con 42 mil millones, y finalmente las tarjetas universitarias destinadas al segmento joven con 19 mil millones.

[5] Mercator Advisory Group, grupo consultor que ofrece servicios de análisis para localizar nuevas oportunidades de mercado y para optimizar iniciativas estratégicas. Trabaja a nivel mundial con la industria bancaria y de pagos. http://www.mercatoradvisorygroup.com/




**Adaptado de Mercator Advisory Group**

Se estima que aproximadamente un 20% de ese mercado global, es decir unos 160 mil millones de dólares, será la proyección para la región de América Latina, siendo Brasil y México los que más cuota abarquen por las características de sus economías y mercados.

En lo que respecta a avances tecnológicos, no se han producido grandes cambios en los últimos años. La mayoría de las tarjetas siguen funcionando con el sistema de banda magnética, mientras que las llamadas "tarjetas inteligentes"—aquellas que poseen un chip con mucha más información que las magnéticas—siguen mostrando un desarrollo menor, limitándose a un uso doméstico y con valores de disposición de capital bajos.

Una de las novedades que sí ha experimentado un importante desarrollo es la asociación de los programas de tarjetas prepagas con los proveedores de servicios de pago móvil o de pago por Internet para ofrecerles a los clientes la posibilidad de tener acceso a efectivo a través de la red global de cajeros automáticos. Estas asociaciones no sólo incrementan mucho más la oferta de ventajas, sino que también fideliza a clientes, y asegura en cierto modo que el sector privado mantenga su margen de beneficios.

Como se indicó anteriormente, los usuarios de las tarjetas prepagas no disponen de cuentas personales individualizadas, sino que es el programa de tarjetas prepagas el que dispone de una cuenta conjunta o "*pooling account*" en un determinado banco. El monto de que se dispone en dicha cuenta es exactamente igual al monto que han comprado (cargado) sus clientes y a medida que éstos realizan operaciones el monto se va reduciendo o incrementando. Al existir una cuenta en un banco, éste está obligado a aplicar medidas de debida diligencia del cliente (DDC) sobre su cliente, es decir el dueño del programa de tarjetas prepagas, pero no tiene la posibilidad de aplicar medidas de DDC a los clientes finales de las tarjetas prepagas pues son clientes del dueño del programa de tarjetas. Esto provoca una carencia de control importante que junto con las características anteriormente descritas del producto, lo convierte en un servicio de alto riesgo de por sí.

No hay que ignorar el hecho de que cuanto más se asemeja una tarjeta prepaga a una cuenta bancaria más riesgos de LA/FT implica, especialmente si estas tarjetas son anónimas, si no se establecen límites de valor, si permiten recargas en efectivo o retiros de dinero en las redes globales de cajeros automáticos. Estas características las convierten en los productos

más anhelados por los criminales, por lo tanto, mientras más similitudes existan con una cuenta bancaria, mayores medidas de mitigación de riesgos habrá que aplicar.

### *2.2 Servicios de Pagos por Telefonía Móvil*

El uso de celulares está volviéndose cada vez con más frecuencia una parte central en la vida diaria de las personas, y no es de extrañar, por consiguiente, que los teléfonos se difundan como un medio de pago alternativo. En los mercados emergentes la movilidad del celular y su amplio alcance territorial están logrando que miles de personas de menores ingresos accedan por primera vez al sistema financiero formal.

Expertos analistas consideran que los pagos móviles—entendidos como transacciones monetarias por celulares—son una tendencia a nivel mundial en proceso de aceleración. Se calcula que entre 2009 y 2010 los usuarios de pago móvil en Latinoamérica pasaron de 5,1 a 8 millones. En Asia se estima que en el 2011 había 62,8 millones de personas usando habitualmente sus teléfonos con fines financieros.[6]

Usando como referencia el informe del Banco Mundial "Integridad en los Servicios Financieros mediante Teléfonos Móviles" publicado en 2008, podemos distinguir cuatro categorías de servicios financieros a través del teléfono móvil.[7] De las cuatro categorías presentadas a continuación, serán las dos últimas las que más nos interese en este informe debido a sus riesgos de LA/FT:

1. **Servicios de información financiera móvil:** en este caso los clientes tienen un acceso extendido a su información financiera a través de sus celulares pero no tienen la posibilidad de realizar operaciones, como por ejemplo transacciones.

2. **Banca móvil:** son servicios que ofrece la entidad financiera a sus clientes a través de sus celulares. No son servicios estrictamente nuevos sino que la entidad financiera ahora facilita una gestión de los mismo pero de forma remota. Entre las operaciones realizables se encuentran: consultas de saldo, transferencia entre cuentas, solicitud de chequeras, suspensión de cheques, pago de facturas, pago de préstamos o la consulta del historial de transacciones.

3. **Monedero móvil:** Funciona como una alternativa al dinero en efectivo. Los clientes pueden almacenar valor en sus celulares, y pueden usar su crédito o tiempo aéreo[8] como método de pago o transferencia. En el momento de la compra, bastará con pasar el código de barras que aparecerá en el teléfono por el lector que tiene instalado el establecimiento. Esta modalidad puede suponer riesgos dependiendo de su funcionalidad y otras medidas mitigadoras que aplique.

4. **Servicios de pagos móviles:** permiten a personas que disponen de cuentas, ya sea con bancos u otras entidades financieras no bancarias, realizar operaciones con teléfonos celulares (pagos en comercios, compras desde el móvil, transferencias

[6] Declaraciones de Diego Pleszowski, socio líder de Consultoría para la Industria Financiera de Ernst & Young, para Diario Financiero, 30 de Mayo 2012, Chile. http://www.eychile.cl/movil/sala-de-prensa/noticias/el-potencial-de-los-pagos-moviles-en-el-desarrollo-economico/

[7] Banco Mundial, Working paper Nr. 146, *Integrity in mobile phone financial services*, Washington, 2008, p. 18. http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf

[8] Tiempo aéreo hace referencia al valor utilizable almacenado en el dispositivo. Muchas operadoras móviles utilizan dicho término en vez de uno monetario.

entre cuentas, pago de facturas, etc.). Cuando los proveedores de servicios son las entidades financieras bancarias se aplican medidas ALA/CFT homogeneizadas, sin embargo, en muchos casos, los proveedores de estos servicios son instituciones financieras no bancarias y pueden no disponer de medidas de control y supervisión adecuadas.

Entre los servicios de pago móvil se pueden diferenciar varios modelos: i) modelo de pago móvil centrado en el banco; ii) modelo de pago móvil centrado en el operador de telefonía móvil (MNO, por su siglas en inglés); y iii) modelo de pago móvil en colaboración.

i) **Modelo de pago móvil centrado en el banco:** En este modelo los clientes disponen de cuentas bancarias que ofrecen el servicio de pago móvil. Los fondos utilizados siempre vienen de una cuenta de un cliente con dicho banco. El MNO en este caso es puramente un canal de transmisión de los avisos de las transacciones pero no influye en las operaciones. Es el banco el responsable, por lo que si el banco cumple con sus requisitos de DDC de forma completa, así como con el registro de transacciones y de reporte de operaciones sospechosas, dicho producto se podría considerar de bajo riesgos.

ii) **Modelo de pago móvil centrado en el MNO:** Con el objetivo de fidelizar a sus clientes y agregarle un valor añadido, los MNOs han comenzado a ofrecer a sus clientes una serie de servicios que anteriormente sólo proporcionaban los bancos, como es el caso del pago móvil. Los MNOs pueden ofrecer cuentas prepagas o pospagas. En la primera, el cliente utiliza el importe que previamente ha recargado, mientras que en la segunda, el cliente usa fondos que posteriormente abonará al MNO durante el período de facturación correspondiente. En este último caso, como el cliente usará el dinero del MNO hay un incentivo implícito para que éste aplique medidas de DDC en su totalidad.

Dentro de este modelo podemos distinguir de forma orientativa servicios de bajo y alto riesgo. Un servicio de bajo riesgo sería por ejemplo la facturación de compras de productos del propio MNO como melodías para el teléfono, juegos u otros productos de comercios pertenecientes a un ciclo cerrado afiliado con el MNO. Un servicio de alto riesgo sería aquel en el que el MNO funciona como un proveedor de servicios de transferencias de dinero o valores (STDV) abierto que permite la realización y recepción de pagos a nivel nacional e internacional—en aquellos casos en los que el MNO tiene socios STDV fuera del país.

En comparación con el modelo de pago móvil centrado en una institución financiera bancaria, el pago móvil centrado en el MNO comporta mayores riesgos (al igual que las tarjetas prepagas), especialmente porque en muchos casos el MNO tiene una cuenta bancaria donde junta todo el capital de sus clientes (pooling account). Si bien el MNO está sujeto a medidas de DDC con el banco donde tiene dicha cuenta, el banco no puede aplicar medidas de DDC sobre los clientes finales del servicio de pago. Tampoco quedan supervisadas las transacciones de dinero en efectivo que se realizan en puntos de venta minoristas o a través de terceros agentes.

iii) **Modelo de pago móvil en colaboración:** En aquellas regiones geográficas menos atendidas por el sistema financiero, los bancos y los MNOs se están asociando para crear redes de agentes que ofrezcan los mismos servicios financieros que en las áreas geográficas

más bancarizadas. Esto promueve una alta inclusión financiera y a su vez fideliza al cliente tanto con el banco como con la compañía de telefonía. Sin embargo, no debe quedar como una asignatura pendiente indicar en este modelo qué parte es claramente la responsable de cumplir con las obligaciones regulatorias ALA/CFT.

Los tres modelos anteriormente mencionados pueden proporcionar acceso a dinero en efectivo a través de sucursales, cajeros automáticos o incluso a través de terceros agentes. El uso de terceros agentes requeriría que éstos tuviesen licencia o estuviesen registrados ante la autoridad competente del país, o que el proveedor de servicios de pago móvil mantuviese una lista exhaustiva y accesible con todos sus agentes. Además, estos agentes deberían estar incluidos en los programas de ALA/FCT de los proveedores y a su vez ser supervisados para asegurar el cumplimiento de sus deberes.

El avance en la tecnología móvil ha ido alcanzando tal sofisticación que los celulares funcionan ya como pequeñas computadoras. En lo que respecta a los pagos, éstos se realizan bien mediante códigos o comandos a través de mensajes de texto o por Internet, o bien a través de un chip adhesivo en el celular que confirma el pago o transacción al pasarlo junto a un aparato lector compatible en el comercio.

En el contexto de estos avances, se destaca la fusión de los sistemas de pagos móvil con STDV tradicionales y otros NMPs ofreciendo servicios tales como:

- Tarjetas prepagas de ciclo abierto que permite a clientes tener acceso a efectivo en cualquier parte del mundo a través de la red global de cajeros automáticos.

- Retirada dinero en efectivo a través de cajeros automáticos sin tener que disponer de tarjeta física y usando tan sólo un código al que se encuentra asociada una cantidad determinada.

- Servicios de remesas mediante los cuales terceras partes que no sean clientes de los proveedores de servicios de pago móviles puedan enviar, recibir y retirar dinero de clientes que usen los servicios de pago móviles.

- Transferencias de tarjeta a tarjeta iniciadas por un teléfono móvil.

### *2.3 Servicios de Pagos por Internet*

Internet ha sido otro ejemplo más de cómo la tecnología se ajusta rápidamente a las necesidades de los humanos hasta el punto de que para muchos sería imposible concebir hoy día un mundo sin Internet. A pesar de que en sus comienzos sólo aquellos con un alto poder adquisitivo se lo podían permitir, hoy en día gracias a nuevas infraestructuras y a precios cada vez más competitivos, Internet es mucho más accesible, y su alianza con otras tecnologías como la telefonía móvil lo han llevado prácticamente a casi todos los rincones del mundo. La gran demanda de Internet y la confianza en su uso ha venido acompañada de la oferta de nuevos servicios que completan las necesidades de los usuarios, como son los pagos a través de Internet.

Hay que destacar que la penetración de Internet en la región latinoamericana no deja de sorprender, a pesar de estar muy lejos de las cifras de otras regiones geográficas. Según datos de la CEPAL, el uso de Internet en América Latina crece a un ritmo sostenido y ha

pasado de una tasa de penetración del 11% a principios del 2000 a más del 30% en pocos años.[9] A esta tendencia hay que añadirle los resultados aportados por analistas que identifican un crecimiento del 13% de las compras en línea durante 2012.[10] Estas cifras nos hacen vaticinar que el uso de otros servicios en línea como los métodos de pago por Internet se expandirán a medio y largo plazo.

Un servicio de pago por Internet es un STDV que permite a sus usuarios realizar operaciones en línea con el dinero virtual que previamente ha sido comprado o cargado en una cuenta prepaga. La estructura de un sistema de pago de este tipo requiere al cliente o usuario que se registre con el proveedor del sistema de pago antes de que el sistema efectúe cualquier transacción. Normalmente el proceso de registro suele requerir—aunque no en todos los casos—la introducción y verificación de alguna información del cliente (E-mail, teléfono, código postal, entre otros) para poderlo dar de alta y proporcionarle un usuario y contraseña para que se conecte y haga uso del sistema. La información requerida dependerá del producto, del tipo de negocio o de la regulación dispuesta en la jurisdicción donde se encuentre.

Una vez activada la cuenta y hecha una recarga de fondos, el cliente podrá utilizarlos en línea, transferírselos a otra persona o extraerlos. Las extracciones pueden tomar la forma de dinero en efectivo si el servicio de pago está asociado con un emisor de tarjetas prepagas. De lo contrario, el cliente o beneficiario de una operación tendrá que usar otras alternativas, como por ejemplo, recibir un cheque enviado por correo o transferir los fondos a otros STDV.

Las cuentas de los sistemas de pago por Internet tienen un formato prepagado, lo que indica que el usuario ha aportado fondos con anterioridad a la operación, y serán exclusivamente estos fondos los que podrá gastar. Existen muchas maneras de recargar estas cuentas. Las cuentas bancarias o las tarjetas de crédito/débito son las más usuales. En términos de lucha contra el blanqueo de capitales estos métodos de financiación son los más efectivos porque siempre dejan un rastro electrónico en el que se encuentran asociados datos de sus usuarios, haciendo consecuentemente más fácil el trabajo de las agencias de investigación y aplicación de la ley. El problema, sin embargo, viene cuando se usan métodos menos rastreables como por ejemplo las tarjetas prepagas o el dinero en efectivo.

El informe del GAFI de 2010 encuadra los métodos de pago por Internet en tres categorías:

a) **Banca electrónica**. Las instituciones crediticias ofrecen acceso en línea a servicios de banca tradicional basados en la cuenta que un cliente dispone con la institución.

b) **Productos de pago por Internet prepagados**. Se trata de firmas—sin necesidad de ser instituciones crediticias—que permiten a los clientes realizar multitud de operaciones a través de cuentas prepagas virtuales a las que pueden acceder por Internet.

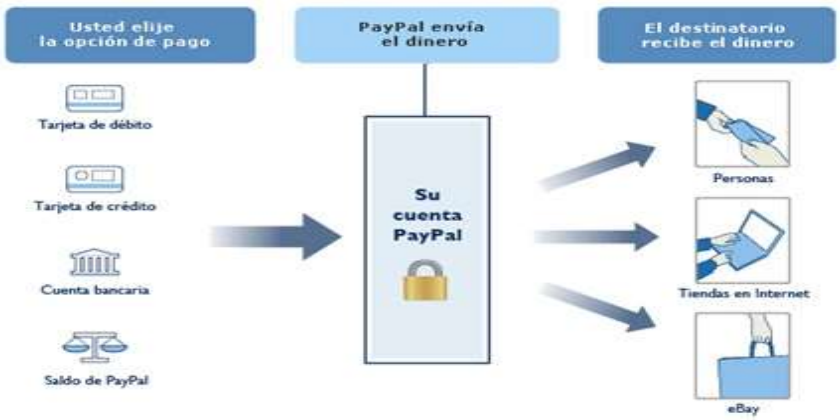
[9] CEPAL, *Avances en el acceso y el uso de las Tecnologías de la Información y la Comunicación en América Latina y el Caribe 2008 – 2010*, Marzo 2010, Santiago de Chile, p. 12. www.eclac.cl/ddpe/publicaciones/xml/3/38923/w316.pdf
[10] Tendencia Financiera, *Usos de Internet en Latinoamérica 2012*, 7 de Noviembre de 2012. www.tendenciasdigitales.com/1461/infografia-usos-de-internet-en-latinomarica-2012/

c) **Monedas o métales digitales**. En este caso los clientes pueden comprar unidades de moneda digitales que pueden luego cambiar con otros clientes de cuentas de la misma naturaleza o cambiarlas por moneda real y realizar retiros en efectivo. En este modelo las unidades de moneda electrónica son emitidas y canjeadas por agentes intermediarios que pueden estar afiliados al proveedor o ser independientes y por lo tanto actuando como una oficina de cambio virtual. Este modelo de negocio adquiere su retribución por cada transferencia que realizan desde sus cuentas a las cuentas de los clientes.

   En muchos casos las monedas digitales están asociadas a mundos virtuales o juegos. El dinero adquirido se usa para realizar operaciones relacionadas con un mundo virtual determinado, con sus jugadores o con minoristas siempre dentro del ámbito online cerrado. En muchos casos estas monedas se pueden canjear por su equivalente en moneda real al salir del juego.

El aumento en el uso de Internet, así como la cada vez mayor aceptación por parte de los comercios de los pagos por este canal han provocado que los productos de pago por Internet crezcan considerablemente y se hayan diversificado permitiendo, por ejemplo, las transferencias de persona a persona (P2P), que son particularmente las que más riesgos de lavado suponen. Además, los servicios de pago por Internet están cada vez más interconectados con los demás servicios de pago, ya sean nuevos o tradicionales, aumentando con creces el abanico de operaciones de que este método dispone para sus usuarios (remesas, transferencias, tarjetas prepagas para acceso a efectivo, etc.). A mayor funcionalidad mayores los riesgos, es por ello que los reguladores deben prestar especial atención en asegurar que se aplican medidas de mitigación de riesgo apropiadas.

**Esquema de pago por Internet mediante PayPal[11]**




[11] Existen muchos otros modelos de pago por Internet como por ejemplo: Google Wallet, Amazon Payments, Money Bookers, entre otros.

## CAPÍTULO 3: RIESGOS

Al igual que cualquier otro producto o servicio financiero, los NMPs no están al 100% exentos de ser utilizados por criminales en operaciones de lavado de activo y financiación del terrorismo. Cada servicio y producto puede contener riesgos distintos, por lo que siempre es aconsejable analizarlos individualmente.

Dentro de la gran diversidad de riesgos que acompañan a los NMPs, el GAFI identificó en su informe de 2006 los siguientes riesgos comunes:[12]

- Ausencia de riesgo de crédito. Los fondos usados son previamente pagados, por lo que los proveedores de servicio están poco incentivados a obtener más información sobre el cliente o el tipo de operación ya que no están en riesgo de perder dinero;

- Velocidad de transacción. Las operaciones se pueden llevar a cabo mucho más rápido que con los canales tradicionales, lo que complica el monitoreo y un posible congelamiento de fondos;

- Relación impersonal. Muchos de los proveedores de NMPs establecen relaciones con clientes sin que ellos estén presente en ningún momento, lo que aumenta el riesgo por identificación falsa.

Muchas jurisdicciones ya han establecido medidas de prevención, control y lucha contra este fenómeno por parte de los proveedores de NMPs, sin embargo, aún queda mucho por hacer. Es imprescindible que las medidas sean percibidas siempre como positivas por todas las entidades interesadas que estén involucradas en el sistema de pago. Por un lado, podrán aportar más transparencia en los pagos por transacciones, y ayudarán a prevenir la corrupción y otros abusos. Por otro lado, propiciarán el deterioro del uso de la secciones ilegales del mercado de pagos como *hawaladars* o los servicios bancarios "clandestinos".

Además, hay que tener en cuenta las ventajas que nos ofrece la naturaleza electrónica de estos métodos de pago a la hora de realizar investigaciones. Las operaciones de los NMPs siempre dejan un rastro electrónico, algo que por el contrario no hace el dinero en efectivo. Incluso sin realizar DDC, se puede obtener información esencial de ese rastro electrónico. A través de la tarjeta SIM del teléfono, o la IP de la computadora, se puede localizar dónde se ejecutó el pago o se retiró el efectivo, y esto puede ayudar a identificar o localizar al sospechoso, por ejemplo, a través del sistema de cámaras.

A continuación se presenta una matriz de riesgo desarrollada por el GAFI en 2006 y actualizada en 2010. A modo ilustrativo, esta matriz pretende identificar, evaluar y entender mejor los riesgos inherentes a los NMPs. Durante la actualización de 2010, se introdujeron algunas modificaciones para que quedasen identificados los riesgos resultantes del diseño del propio producto, y los riesgos que derivan de la aplicación de DDC por parte de los proveedores. Acorde con los nuevos estándares aprobados en 2012 se actualiza la numeración de las recomendaciones señaladas en la matriz.

[12] FATF Report, *New Payment Methods*, Octubre de 2010, París. http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

Los factores de riesgo enumerados en la siguiente matriz no deben ser considerados de forma aislada sino como parte de un todo, por lo tanto, el resultado de un factor no debe derivar en un juicio radical simplista sobre el propio producto.

### *3.1 Matriz de Riesgo*

| **Factores de riesgo de los métodos de pago**[13] | | | | |
|---|---|---|---|---|
| **Criterios** | | **Dinero en Efectivo** | **Alto Riesgo** | **Bajo Riesgo** |
| **Debida Diligencia del Cliente** | Identificación | Anónima | Anónima | Los clientes están identificados |
| | Verificación | Anónima | La identidad del cliente (en caso de obtenerse) no está verificada sobre la base de información, datos o documentos de fuentes independientes y confiables | La identidad del cliente se encuentra verificada sobre la base de información, datos o documentos de fuentes independientes y confiables (Rec. 10) |
| | Monitoreo | Ninguno | Ninguno | Monitoreo constante de las relaciones comerciales |
| **Mantenimiento de registros** | | Ninguno | Se generan registros de la transacción, pero no son conservados ni son puestos a disposición del organismo de aplicación de la ley | Los registros de la transacción son conservados y puestos a disposición del organismo de aplicación de la ley |
| **Límites de valor** | Máximo monto almacenado en cuenta/s por persona | Sin límite | Sin límite | Monto límite |
| | Máx. monto por transacción (incluso de carga / retiro) | Sin límite | Sin límite | Monto límite |
| | Máx. frecuencia transacción | Sin límite | Sin límite | Transacción límite |
| **Métodos de financiación** | | No aplicable | Fuentes anónimas de financiación (Ej. efectivo, órdenes de pago, NMPs anónimos); también múltiples fuentes de fondos, ej. terceras partes | Aporte de fondos a través de cuentas abiertas en una institución financiera o de crédito regulada, u otras fuentes |

[13] GAFI Report, *Money Laundering Using New Payment Methods*, Octubre 2010, París, pp. 22-23. http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

| | | | | |
|---|---|---|---|---|
| | | | | identificadas sujetas a obligaciones de y fiscalización adecuadas en materia ALA/CFT |
| **Alcance geográfico** | | Algunas monedas son aceptadas en forma más generalizada que otras; las monedas pueden ser convertidas a través de intermediarios | Transferencia de fondos o retiro a través de fronteras nacionales | Transferencia o retiro de fondos sólo a nivel nacional |
| **Límites de uso** | Negociabilidad (aceptación del comerciante) | Generalmente aceptada | Gran cantidad de comerciantes y puntos de venta que aceptan (Ej. a través del uso de las normas de VISA o MasterCard) | Poca cantidad de comerciantes y puntos de venta que aceptan |
| | Utilidad | No es posible el uso virtual para operaciones p2b, b2b, p2p[14] | Es posible el uso virtual para operaciones p2b, b2b, p2p | Es posible el uso virtual en p2b, b2b, pero no para p2p |
| | Retiro | No aplicable | Retiro anónimo e ilimitado (Ej. efectivo por cajeros automáticos) | Opciones de retiro limitadas (Ej. únicamente en cuentas de referencia); montos de retiro y frecuencia limitados (Ej. menor a un determinado monto fijo por año calendario) |
| **Segmentación de servicios** | Interacción de proveedores de servicios | No aplicable | Varios proveedores de servicios independientes que ejecutan pasos individuales de la transacción sin una supervisión y coordinación eficaces | Toda la transacción es llevada a cabo por un solo proveedor de servicios |
| | Tercerización | No aplicable | Varios pasos son tercerizados; tercerización en otras jurisdicciones sin resguardos apropiados; falta de supervisión y de claras líneas de responsabilidad | Todos los procesos son cumplidos internamente conforme a los más altos estándares |

[14] Transacciones p2b (de persona a negocio), b2b (de negocio a negocio) y p2p (de persona a persona).

### *3.2 Evaluación de Riesgos*

La matriz anterior permite tener una visión clara de las principales amenazas que acompañas a los NMPs. En pos de un mejor entendimiento, se presentan a continuación de forma individualizada cada uno de los riesgos identificados.

#### *3.2.1 Debida Diligencia del Cliente*

Una de las claves de las medidas DDC es asegurar que las instituciones financieras puedan identificar, verificar y monitorear de forma efectiva a sus clientes y las operaciones que éstos realizan. Durante mucho tiempo, el sector bancario las ha aplicado obteniendo como resultado la disminución del fraude y el delito. Sin embargo, cuando se trata de los NMPs, la aplicación de estas medidas se complica debido a las características intrínsecas de que gozan y que en definitiva son la razón de ser del propio producto.

Las tarjetas prepagas, por ejemplo, al mismo tiempo que mantienen su total grado de funcionalidad, ofrecen al cliente un absoluto anonimato. No se requiere identificación alguna. De hecho, muchos emisores de tarjetas van más allá, y utilizan en sus campañas publicitarias el carácter "anónimo" como argumento para atraer clientes. Un anonimato que, además, se puede dar en distintas fases del producto (la adquisición, recarga, transferencia, etc.) y que imposibilita cualquier intento de rastreo. Ni siquiera tienen una cuenta bancaria personal relacionada a través de la cual se pueda acceder a los datos del cliente, por lo que éste puede simplemente recargar con efectivo desde cualquier lugar autorizado y difícilmente podrá ser rastreado. Las tarjetas pueden operar sin problemas en todo el mundo a través de las redes globales de cajeros automáticos; en algunos casos pueden incluso sustituir a los servicios de envío de remesas tradicionales, por ejemplo, en el caso de las "tarjetas gemelas". Al existir dos tarjetas, dos usuarios distintos pueden usar los fondos de la misma cuenta sin que importe la localización. Podemos inferir que el anonimato es un catalizador de los riesgos que implica la funcionalidad de las tarjetas.

> En 2007, dos demandados fueron acusados en EE.UU. de blanqueo de dinero en conexión con la transferencia de ganancias por tráfico de drogas a Colombia a través de la red de cajeros automáticos. Los acusados dieron directivas a sus familiares y amigos a que abrieran cuentas bancarias donde ingresaban entre 500 o 1500 dólares. Por cada cuenta sacaban dos tarjetas gemelas, una se la quedaban ellos y la otra la enviaban a Colombia donde se retiraba el efectivo a través de cajeros.[15]

Poder aplicar medidas de DDC e identificar los casos de fraude de identidad es muy difícil para los proveedores de NMPs debido a la tan despersonalizada relación con el cliente. Este tipo de relación es común en los servicios de pago por Internet donde las actividades de negocios son exclusivamente virtuales. Los sistemas de identificación y verificación de clientes de estos servicios de pago no son homogéneos. Si bien algunos pueden tener sistemas sofisticados en los que se piden datos personales tales como cédula de identidad, dirección, nombre completo, etc., y se verifican usando bases de datos de terceros, la mayoría no requiere más que datos que no dicen realmente nada de la persona que está realizando las operaciones, como un nombre, pseudónimo o un correo electrónico.

[15] FATF Report, *New Payment Methods*, Octubre de 2010, París, p. 46. http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

Los servicios de pago móvil también presentan el mismo riesgo que en los pagos por Internet cuando la relación comercial no se establece a través de agentes sino en línea. Un agente brinda a las instituciones la posibilidad de llevar a cabo DDC mientras el cliente se encuentra físicamente presente ya que puede verificar in situ la documentación e identidad del mismo. En cambio, al utilizar Internet, el proveedor de servicios móviles deberá depender de una identificación y verificación a distancia. Los riesgos de este servicio dependerá en gran medida de la funcionalidad que ofrezca y las medidas de mitigación de riesgos que ya aplique. En cualquier caso, la carencia de identificación y verificación supondrá altos riesgos de uso para fines ilícitos.

Otro riesgo que afecta a la aplicación de DDC en los NMPs se presenta con la existencia de "*pooling accounts*" o cuentas conjuntas. Los proveedores de estos servicios de pagos pueden abrir cuentas en bancos donde unifican todo los capitales de sus clientes. En términos legales el cliente del banco, es decir el proveedor de servicios, tiene que estar sujetos a medidas DDC del propio banco, pero el banco sólo tendrá responsabilidad para con el proveedor y no para con los clientes que usan los servicios ofrecidos por el proveedor. Este esquema deja una laguna de control y supervisión que contempla graves riesgos de LA/FT.

### *3.2.2 Mantenimiento de Registros*

El mantenimiento de registros es imprescindible para reconstruir las transacciones en caso de investigaciones

En conformidad con la Recomendación 11 del GAFI, "*debe exigirse a las instituciones financieras que mantengan, por un período de al menos cinco años, todos los registros necesarios sobre las transacciones, tanto locales como internacionales, para que éstas puedan cumplir con rapidez con las peticiones de información solicitadas por las autoridades competente.*"

Los registros deben ser suficientes para permitir la reconstrucción de las transacciones con el fin de suministrar las pruebas necesarias para el procesamiento de la actividad delictiva. Algunos de los registros necesarios de las transacciones son: "*nombre del cliente (y del beneficiario), dirección (u otra información identificativa normalmente registrada por el intermediario), carácter y fecha de la operación, el tipo y el monto de la moneda involucrada, y la clase y número identificativo de todas las cuentas involucradas."*

Aunque la Recomendación 11 especifica la necesidad de que se mantengan registros, surgen algunas controversias al intentar aplicar esta recomendación a los NMPs. Las tarjetas prepagas, por ejemplo, permiten un total anonimato, haciendo que no se conozca necesariamente quién origina la transacción, quién es el beneficiario, o cuál es el carácter de la operación. Consecuentemente, impide el mantenimiento de registros con información básica necesaria para una eventual investigación por casos de LA/FT, por lo que promueve el potencial uso de esta medio de pago en operaciones con fines ilícitos.

En el caso de los pagos móviles o pagos por Internet, además de que difícilmente se obtienen datos de la aplicación de DDC, tampoco requieren el mantenimiento de datos

únicos como son la IP para los pagos por Internet, o el número de celular y el número de la tarjeta SIM en las transacciones mediante servicio móvil.

### *3.2.3 Límites de Valor*

Cuanto más alto sea el valor y la frecuencia de las transacciones permitidas, así como el valor en cuenta y la ausencia de límites, mayores serán los riesgos de blanqueo de capitales y financiación del terrorismo.

La aplicabilidad del término ¨límites de valor" tiene gran alcance; ésta abarca límites en el máximo importe que puede hallarse depositado en una cuenta o producto de NMP, restricciones en el monto máximo por operación de pago único, límites en la frecuencia o valor de las operaciones permitidas en un intervalo de tiempo determinado, o en el número de cuentas o productos a los que puede acceder un titular, e incluso una combinación de las restricciones antes mencionadas.

En la actualidad existe amplia diversidad en lo que respecta a los límites de valor en los productos de los NMPs. Normalmente, los servicios de pago móvil ofrecen límites de valor estrictos, lo que dificulta su uso para fines ilícito. No obstante, no siempre ocurre así con los otros NMPs; por ejemplo, si bien existen tarjetas prepagas no recargables con valores bajos como 100 dólares, existen otras que son recargables y tienen altos límites de valor como 30.000 dólares mensuales.

No es de extrañar que la mayor parte de los proveedores de productos con escasos límites de valor—o sin límites—se encuentren en jurisdicciones donde los NMPs no están apropiadamente regulados ni supervisados. Por un lado, aseguran sus ventas al ofrecer productos con características muy atractivas (privacidad, límites de valor poco estrictos, carencia de impuestos, etc.); por otro lado, no encuentran restricciones geográficas ya que venden la gama de sus productos a través de agentes intermediarios o por Internet.

### *3.2.4 Métodos de Financiación*

Los NMPs permiten financiar sus productos de muchas formas distintas, lo que viene a considerarse una ventaja para los clientes. Sin embargo, no todo son ventajas cuando nos referimos a riesgos de LA/FT. Por un lado, siempre que exista una cuenta bancaria asociada al cliente los riesgo de LA/FT se reducen notablemente al estar sujetos a controles por parte de la entidad financiera; desafortunadamente, a pesar de que tener una cuanta bancaria asociada sería lo ideal, actuaría al mismo tiempo de forma contraproducente al actuar en detrimento del público no bancarizado. Por otro lado, cuando el cliente decide aportar fondos usando dinero en efectivo o sistemas no bancarios, el acceso al público se incrementa, pero también lo hacen los riesgos de LA/FT, ya que el efectivo es anónimo, y al no poderse rastrear permite saltarse controles con facilidad; del mismo modo ocurre con el uso de otros servicios de pagos basados en una cuenta que no verifica la identidad del cliente, o con los servicios que facilitan transferencias de cuenta a cuenta y que permiten la financiación a través de terceros.

### *3.2.5 Límite Geográfico*

Mientras mayor alcance geográfico tenga un producto para realizar pagos, retiros de efectivo o transferencias de fondo, más riesgo de LA/FT existirán.

Teniendo en cuenta la diversidad de servicios que ofrecen, las tarjetas prepagas son las que más riesgos comprenden, ya que permiten que sus usuarios realicen pagos, retiren efectivo, o envíen y reciban fondos a través de los principales circuitos de pago internacionales. Además, su tamaño proporciona particular atractivo para muchos delincuentes que ya no tienen que cruzar fronteras con grandes montos en efectivo. Además de la movilidad transfronterizas de las tarjetas, no existe forma de verificar el saldo contenido. Estados Unidos ha presentado algunas enmiendas a su *Bank Secrecy Act* para que la Red contra los Delitos Financieros (FINCEN) pueda requerir que los viajeros declaren el valor de sus tarjetas en puntos de entrada del país y se utilicen lectores de tarjetas especiales que indiquen los montos disponibles.[16]

En el caso de los servicios de pago móvil, aunque no existe aún un servicio global, existen proveedores que ofrecen pagos transfronterizos con algunos países en cuestión (Reino Unido-Kenia, Filipinas-Malasia). Algunos proveedores han expandido sus posibilidades asociándose con negocios de remesas, u ofreciendo la posibilidad de conectar con la red global de cajeros automáticos para sacar dinero con tarjetas prepagas o códigos asociados a una cantidad de efectivo concreta.

En el caso de los servicios de pago por Internet, el riesgo se materializa cuando los negocios se pueden realizar desde jurisdicciones donde no hay una regulación o supervisión de ALA/CFT adecuada, por lo que las transferencias transfronterizas pueden fácilmente esquivar cualquier tipo de control y permanecer ocultas e impunes en caso de investigaciones.

### *3.2.6 Límite de Uso*

Mientras menores sean los límites de uso y mayor el número de operaciones distintas permitidas por los productos, mayores serán los riesgos de que los criminales exploten los NMPs para fines ilícitos.

Los límites de uso hacen referencia a la cantidad de operaciones distintas que un producto de NMPs puede realizar; sus riesgos de LA/FT son proporcionales a su funcionalidad.

El caso de las tarjetas prepagas es algo peculiar. Las tarjetas están mundialmente aceptadas y pueden ser usadas para muchos tipos de operaciones diversas. Estas características impiden la imposición de grandes límites de uso lo que conlleva a su vez mayores riesgos de LA/FT. Un claro ejemplo es el hecho de que una tarjeta prepaga permita el acceso a dinero en efectivo a través de la red internacional de cajeros automáticos: los fondos cargados en una tarjeta prepaga pueden ser extraídos en otro país. Es decir, los delincuentes pueden introducir el dinero procedente de delitos en el sistema bancario y sacarlos en otro

[16] FINCEN, http://www.fincen.gov/statutes_regs/frn/pdf/FR_monetary_instrument.pdf

país, blanqueándolos y ahorrándose el transporte de grandes sumas de dinero en efectivo. Algunos países como los Estados Unidos ha intentado controlar el transporte transfronterizo de estas tarjetas y han desarrollado un lector que puede averiguar cuanto dinero contiene la tarjeta; aún así esta tecnología se está implementando poco a poco en zonas de frontera.

Los servicios de pago móviles o por Internet tienen mayores límites de uso. Aunque no estrictamente de forma generalizada, normalmente las transacciones de pago se realizan entre clientes del mismo proveedor o permiten pagos de sumas muy pequeñas por lo que el riesgo es notablemente menor. No ocurre lo mismo cuando estas modalidades se asocian con otros NMPs para ofrecer más servicios puesto que se incrementan las operaciones posibles y, por consiguiente, también propician que existan más fallas que los criminales puedan explotar.

### *3.2.7 Segmentación de Servicios*

Cuanto mayor sea el número de partes involucradas en la ejecución de un servicio de pago, mayor será el riesgo de pérdida de información de clientes y de transacciones, y por lo tanto, de LA/FT.

Las partes involucradas en un servicio de pago son muy diversas: emisores de tarjetas, gerentes de programas, agentes de cambio, red de pagos, distribuidores y otros tipo de intermediarios o mandatarios, proveedores de servicios de pago internacionales, etc.

Los proveedores de servicios que manejan todos los aspectos de la relación comercial (registro, ingreso y salida de dinero, transacciones, etc.) pueden representar un menor riesgo que los servicios descentralizados ya que las autoridades competentes pueden fácilmente localizar y monitorear las políticas y procedimientos ALA/CFT del proveedor de servicios.

La situación de riesgo se ve en cambio exacerbada en aquellos casos donde se produzca una delegación de funciones a terceros no regulados, que no tengan claras líneas de responsabilidad y/o fiscalización, o que se encuentren en jurisdicciones con poco control o supervisión en temas de LA/FT. En la mayoría de las jurisdicciones los mandatarios no están bajo supervisión alguna o tienen una supervisión limitada; además, éstos no pueden ser sancionados por infringir obligaciones de LA/FT porque las responsabilidades siguen recayendo sobre los proveedores de NMPs. Es muy difícil para los proveedores controlar que sus mandatarios estén eficientemente entrenados, que cumplan con las medidas ALA/FCT requeridas y que informen a las autoridades competente de forma correcta de operaciones sospechosas, especialmente cuando se encuentran en el extranjero o cuando los mandatarios hacen uso de sub-mandatarios.

El riesgo que deriva de la segmentación se ve altamente acentuado en los servicios de pago por Internet por su naturaleza virtual y transfronteriza. Por ejemplo, en los servicios de compra y venta de moneda digital, el proveedor no tiene contacto con el cliente sino que es el cliente quien compra al intermediario, y éste le transfiere el importe determinado de la moneda. Se produce una alta falta de control que puede fácilmente derivar en operaciones ilícitas.

A veces tampoco está claramente establecido cuáles de las entidades involucradas se encuentran sujetas a las obligaciones ALA/CFT o cuáles de todas las jurisdicciones involucradas en el proceso de la transacción son competentes para regular, supervisar y garantizar el cumplimiento de dichas medidas.

### *3.3 Medidas de Mitigación de Riesgos*

Una vez se ha entendido la naturaleza y funcionamiento de estos productos y las amenazas comprendidas en ellos, se puede pasar a atender en detalle algunas medidas de mitigación de riesgos identificados por el GAFI.

Es importante partir de la premisa de que el riesgo de un producto es el resultado de la combinación de todos los riesgos analizados en el apartado anterior. Se entiende, por lo tanto, que la mitigación de riesgo más efectiva es también aquella con un enfoque individualizado, ajustado y proporcional al nivel de riesgo de un producto concreto. Estas medidas de mitigación son imprescindibles para que las instituciones financieras las tenga en cuenta en las primeras fases del diseño de sus productos.

Para poder conseguir minimizar las amenazas de LA/FT a sus niveles más bajos, es preciso atender en primer lugar a la Recomendación 1 del GAFI. Dicha recomendación sugiere a los países que deben identificar, evaluar y entender sus riesgos de LA/FT para ajustar sus regulaciones y requerir a las instituciones financieras que las implementen estableciendo procesos de identificación, evaluación, monitoreo, administración y mitigación de riesgos.

La aplicación de un enfoque basado en el riesgo permite que en los casos en los que se identifiquen riesgos mayores, los países puedan asegurar que sus regímenes ALA/CFT los abordan y que se toman medidas intensificadas para manejarlos y mitigarlos. En aquellos casos en los que se identifiquen riesgos menores, los países pueden tomar la decisión de permitir medidas simplificadas de algunas de las recomendaciones del GAFI. En ocasiones estrictamente limitadas y justificadas donde exista un bajo riesgo probado de LA/FT, o donde una persona natural o jurídica lleve a cabo una actividad financiera de manera ocasional o muy limitada, los países pueden tomar la decisión de aplicar exenciones a algunas de las recomendaciones del GAFI para las instituciones financieras.

En relación con el enfoque basado en el riesgo descrito por la Recomendación 1, se encuentra la Recomendación 15, aunque ésta última se centra exclusivamente en los riesgos que puedan surgir con respecto al desarrollo de nuevos productos, nuevas prácticas comerciales, nuevos mecanismos de envío, uso de nuevas tecnologías, o tecnologías en desarrollo. Esta recomendación, que afecta directamente a los NMPs, indica que las instituciones financieras deben prestar especial atención a las nuevas tecnologías para poder mitigar lo riesgos en las fases de diseño de los productos.

Teniendo en cuenta estas recomendaciones se puede realizar una aproximación más coherente a las medidas de mitigación. En definitiva, permite aplicar una versión más flexible de controles que hacen que los productos sean aún viables y más seguros.

A continuación se describen las medidas de mitigación de riesgo que el GAFI ha ido destacando en sus estudios desde 2006 a la actualidad y que sirven como guía para este documento.

### *3.3.1 Debida Diligencia del Cliente*

Según la Recomendación 10, no sólo se le prohíbe a las instituciones financieras que mantengan cuentas anónimas o con nombres ficticios, sino que además, se les requiere la aplicación de medidas de DDC cuando: i) establecen relaciones comerciales; ii) realizan transacciones ocasionales por encima de 15,000 USD/EUR o quedan encuadradas dentro de las circunstancias que aborda la Nota Interpretativa de la Recomendación 16; iii) existe una sospecha de lavado de activos o financiación del terrorismo; iv) existen dudas sobre la veracidad o idoneidad de los datos de identificación del cliente previamente obtenidos.

Los proveedores de NMPs están sujetos al cumplimiento de la Recomendación 10 desde que se establece una relación comercial. Se requerirá por lo tanto que entre sus medidas de DDC se identifique y verifique la identidad del cliente y del beneficiario final, que se entienda la naturaleza de la relación comercial, y que se mantenga un monitoreo continuo de dicha relación. La aplicación de estas medidas ayudará a asegurar que las instituciones financieras puedan identificar, verificar y monitorear de forma efectiva tanto a sus clientes como a las operaciones que éstos realizan.

Las medidas de DDC son consideradas unas de las medidas más efectivas para mitigar los riesgos de LA/FT, además, permiten una flexibilización en la aplicación de medidas, dependiendo de los resultados de un enfoque basado en el riesgo realizado previamente; aquellos productos o servicios identificados con alto riesgo tendrán que aplicar medidas de DDC intensificadas mientras que aquellos que son clasificados con bajo riesgo podrán aplicar medidas simplificadas, permitiendo requerimientos de identificación, verificación y monitoreo menos intensivos.

Existen diversos criterios para determinar si aplicar menores o mayores medidas de DDC sobre productos o servicios; la funcionalidad o el alcance geográfico pueden ser algunos de ellos. Mientras más alta sea la funcionalidad o el alcance, mayores los riesgos y por lo tanto mayores serán las medidas de DDC.

Otro criterio para determinar el grado de las medidas de DDC que deben aplicarse es la forma en que se establecen la relación comercial y la identificación del cliente. En los casos en que estos procesos no se lleven a cabo cara a cara habrá que buscar alternativas efectivas para verificar que los datos aportados no son fraudulentos; para ello se pueden usar bases de datos de terceros o el rastreo de la IP única del equipo usado por el cliente. También en aquellas jurisdicciones que carezcan de documentos de identificación apropiados habrá que implementar estrictas medidas de monitoreo de operaciones y actividades sospechosas en combinación, además, con otras medidas de mitigación como por ejemplo los límites de valor.

Los agentes o distribuidores que actúen en nombre de los proveedores de servicios de pago durante el establecimiento de la relación comercial, como ocurre en el caso de los pagos móviles o tarjetas prepagas, deberán realizar los controles de DDC ellos mismos; en estos casos, los agentes o distribuidores deben estar contemplados dentro de los programas ALA/FCT de los proveedores y deben ser monitoreados y supervisados en el cumplimiento de sus requerimientos.

### *3.3.2 Mantenimiento de Registros*

El mantenimiento de registros de transacciones y de DDC ha demostrado ser muy beneficioso para el enjuiciamiento de actividades criminales. Los registros deben ser suficientes para permitir la reconstrucción de transacciones individuales y deben mantenerse durante 5 años.

En el caso de las servicios de pago por Internet, a pesar de que la Recomendación 11 no contiene una instrucción expresa que ordene a las instituciones reunir y llevar un registro de las direcciones IP de sus clientes, es importante notar la importancia de este dato único para las investigaciones de las agencias de aplicación de la ley. De igual modo, se debe incluir en los pagos iniciados por teléfono móvil los números de teléfono y de la tarjeta SIM del originador y del beneficiario, ya que son datos únicos de una operación móvil y pueden servir para averiguar la localización exacta de los teléfonos en caso de que sea requerido.

### *3.3.3 Límites de Valor*

Los umbrales de valor son una buena alternativa para minimizar riesgos al mismo tiempo que se mantienen las ventajas de los servicios o productos. Los límites se pueden aplicar a transacciones, operaciones, recargas, monto acumulado en cuenta, frecuencia de operaciones, etc.

Es preciso especificar que para que los límites sean efectivos y puedan en consecuencia reducir los riesgos de LA/FT, debe existir un monitoreo eficiente de las operaciones para evitar acciones como los esquemas de estructuración u operaciones incongruentes con la naturaleza del propio producto. Los límites de valor podrían estar vinculados a los requerimientos de DDC tras la aplicación de un enfoque basado en el riesgo del producto. De este modo se pueden imponer límites estrictos cuando el nivel de aplicación de las medidas de DDC sea bajo, y límites menos estrictos o ningún límite cuando el nivel de aplicación de las medidas de DDC sea alto.

Existen muchas tarjetas que ya disponen de estos límites y han demostrado que siguen siendo ventajosas para aquel nicho de la población no bancarizado. En el caso del pago móvil, los riesgos son menores porque las cantidades que permiten operar son pequeñas. Le sería muy costoso a un delincuente hacer uso de este método para lavar grandes cantidades de dinero. Aún así, no significa que estén totalmente exentos de riesgos. En el caso de los pagos por Internet no se conoce en general la aplicación de muchos límites de valor; el cliente es libre de cargar y usar lo que quiera.

### *3.3.4 Límites Geográficos*

Algunos proveedores de servicios de NMPs permiten realizar operaciones transfronterizas a sus productos y servicios lo que agrega un gran valor añadido para los clientes a pesar de que las operaciones transfronterizas supongan más riesgos de LA/FT que cuando sólo se pueden realizar a nivel nacional. Es muy conveniente para el cliente poder realizar transacciones internacionales o poder recargar en un país y poder sacar dinero efectivo en

otro, pero también es arriesgado en términos de LA/FT. Si no existen controles estrictos o límites de valor razonables, los riesgos se disparan. Además, muchos proveedores de servicios pueden aprovechar las lagunas regulatorias y establecerse en jurisdicciones con bajos controles de LA/FT quedando fuera del alcance de posibles investigaciones.

Si bien es improbable que se restrinja el uso transfronterizo en el futuro debido a las demandas del mercado, sería interesante que se realizasen controles ALA/CFT tanto en el país donde se origine la operación como donde se reciba (como en los pagos móviles donde dos MNOs deben cooperar para establecer la interoperabilidad que permita el servicio transfronterizo). Los países deben dejar muy claro quiénes son los responsables de aplicar las medidas de ALA/CFT en sus jurisdicciones. Podría ser muy útil también requerir a los proveedores que estén registrados en todas aquellas jurisdicciones donde operen; de esta manera los reguladores tendrán constancia de las acciones que realizan.

### *3.3.5 Métodos de Financiación*

Los métodos de financiación comprenden riesgos en aquellos casos en que se utiliza dinero en efectivo u otros métodos de pagos con carácter anónimo que dificultan el rastreo de su origen. Si bien no se puede suprimir totalmente el uso de efectivo se puede tener en cuenta a la hora de crear el producto y ajustarlo a su propia naturaleza. Por ejemplo, se puede poner un límite máximo de recarga con efectivo u otro método de pago anónimo; en los casos en que los clientes quieran sobrepasar estos límites, los clientes tendrán que aportar más información susceptible de ser verificada por los proveedores de servicios, o bien usar sistemas de pagos tradicionales que ya disponen de por sí de controles ALA/CFT.

### *3.3.6 Monitoreo de Transacciones*

El monitoreo continuo de las operaciones y transacciones ayuda a identificar transacciones, esquemas o cualquier otra operación sospechosa. Sería preciso que los proveedores de servicios implementasen sistemas de monitoreo capaces de detectar actividades sospechosas teniendo en cuenta los riesgos que suponga el cliente, su localización geográfica, las características del producto y el canal de transacción. Este sistema de monitoreo además puede ser útil para detectar clientes haciendo uso de esquemas de estructuración, como por ejemplo, un cliente con numerosas tarjetas prepagas. Del mismo modo, los proveedores podrán apreciar aquellas operaciones que se escapan a la naturaleza del propio producto, por ejemplo, aquellos casos en los que los NMPs son usados como cuentas bancarias (por ejemplo haciendo transferencias de alto valor), pues iría contra la propia naturaleza del producto; no tendría sentido que un cliente usase una tarjeta prepaga para transacciones de alto valor si lo normal por seguridad sería usar una cuenta bancaria.

El sistema de monitoreo puede ir acompañado de sistemas de alerta que actúen automáticamente como indicadores de actividades sospechosas, por ejemplo:

- Cuando existan discrepancias entre la información aportada por el cliente y la información detectada por los sistemas de monitoreo;
- Cuando una cuenta siempre reciba fondos aportado por terceras personas;
- Cuando una cuenta reciba fondos de terceros y automáticamente estos fondos sean transferidos a otras cuentas o sacados en efectivo desde cajeros automáticos;

- Cuando se realizan múltiples retiros de efectivo desde cajeros automáticos;
- Cuando las cuentas de los NMPs se usan sólo para retirar efectivo y no para realizar compras electrónicas;
- Cuando existen numerosas cuentas a nombre del mismo cliente.

Poder analizar esa información junto con los registros mantenidos ayudará a considerar si las operaciones sospechosas tienen un fundamente válido como para ser remitidas como reportes de operaciones sospechosas a las autoridades de inteligencia financiera para que las investiguen.

# CAPÍTULO 4: TIPOLOGIAS

En 2010, el GAFI identificó casos reales que ilustran los riesgos de LA/FT que acompañan a los NMPs. En este informe se presenta una pequeña selección de ellos. Aunque el grupo de trabajo considera que los NMPs también pueden ser usados en operaciones de FT, no encontraron casos directos, por lo que todos los casos se producen en esquemas de LA. Se identificó, sin embargo, un caso de "sospecha" de FT (ver caso 3).

Las tipologías descritas son las siguientes:

- Uso de terceras partes para la financiación;
- Explotación de las operaciones impersonales;
- Complicidad de los proveedores de los NMPs o sus empleados.

El grupo optó por no añadir una cuarta tipología que atendiera al carácter "anónimo" del producto. Sólo encontraron tres casos de anonimato directo en el que el producto no requería identificación o verificación alguna.

## *4.1 TIPOLOGÍA 1: Aporte de fondos por terceras partes*

### A) Tarjetas Prepagas

**Caso 1.** Lavado de ganancias ilegales provenientes de apuestas mediante el uso de tarjetas prepagas (2007).

En este caso se abrían cuentas de tarjetas prepagas para poder hacer en ellas las transferencias de las ganancias. Además, estas tarjetas no tenían que salir de ningún país, ya que tan sólo se enviaban los datos de las tarjetas y éstos eran utilizados para hacer compras por Internet o por teléfono. El negocio virtual de apuestas arrojó ganancias mensuales por un valor aproximado de USD 100.000.

Fuente: Estados Unidos

**Caso 2.** Pago de drogas mediante el uso de tarjetas prepagas (2009).

Una banda de narcotraficantes en una prisión federal recibía el dinero de la droga en cuentas prepagas que otros miembros de la banda en el exterior previamente abrían a sus nombres. Los presos que querían conseguir droga sólo tenían que indicarle a sus familiares que abonaran cantidades determinadas en las cuentas de las tarjetas prepagas.

Fuente: Estados Unidos

**Caso 3.** "Posible" utilización de tarjetas prepagas para la financiación del terrorismo.

Un padre y un hijo sospechosos de actuar como remeseros de dinero fueron encontrados con gran cantidad de tarjetas prepagas que eran recargadas desde distintos lugares en Italia y cuyos fondos eran automáticamente retirados. Parte de esos fondos se transferían a una

cuenta del padre, la cual recibía también otras transferencias desde Pakistán, y el fondo de esta cuenta se usaba a su vez para otras transferencias electrónicas. Se supo que tanto el padre como el hijo habían participado en los ataque terroristas de Mumbai en 2008.

Fuente: Italia

### B) Servicios de Pago por Internet

**Caso 4.** Utilización de un servicio de pago por Internet para el movimiento de ganancias ilícitas obtenidas de la venta de mercadería robada desde un sitio web comercial.

Un individuo robó y compró mercadería robada y la vendió en un sitio web comercial durante tres años. Las ganancias pasaban a través de una cuenta de servicios de pago por Internet asociada a las cuentas de los usuarios del sitio web comercial desde el que operaba. Se estima que obtuvo unas ganancias de aproximadamente USD 459.000.

Fuente: Canadá

### C) Servicios de Pago Móvil

**Caso 5.** Sospecha de uso de pago móvil para el movimiento de fondos asociados con fraude a través de mercadeo por teléfono.

Las víctimas recibieron mensajes de texto que les informaban de haber resultado ganadores en una rifa electrónica y que para poder recibir el premio debían enviar una suma mediante un proveedor de pago móvil para cubrir el gasto de los impuestos relacionados con los premios.

Fuente: Filipinas

**Caso 6.** Venta de crédito telefónico robado a través de pago móvil de persona a persona (2010).

Un individuo utilizó la información robada de tarjetas de crédito para obtener crédito telefónico de manera ilícita que posteriormente vendió a través de servicios de pago móvil de persona a persona.

Fuente: Oficina del Ministerio Público de las Islas Caimán

## *4.2 TIPOLOGÍA 2 Explotación de la naturaleza impersonal de las cuentas de NMPs*

### A) Tarjetas Prepagas

**Caso 7.** Lavado de ganancias robadas de cuentas bancarias de individuos (2007).

Seis demandados fueron acusados de usar información robada mediante un programa informático gratuito para transferir fondos de manera ilegal desde cuentas bancarias robadas a las de ellos mismos, incluyendo tarjetas prepagas. Parte de los fondos

transferidos se usaban posteriormente para cargar fondos en cuentas prepagas que usaban para hacer compras.

Fuente: Estados Unidos

**Caso 8.** Lavado de ganancias provenientes de actividades de *phising* mediante el uso de tarjetas prepagas.

En este caso los delincuentes robaron la identidad de los titulares de cuentas bancarias para hacer transferencias a tarjetas prepagas que funcionaban como cuentas de tránsito. Posteriormente se realizaban retiros en efectivo en cajeros automáticos por la misma cantidad robada.

Fuente: Italia

**Caso 9.** Uso de "empleados fantasma" para el lavado de fondos ilícitos mediante el uso de tarjetas prepagas (2009).

Un demandado fue acusado por la malversación de fondos de su empleador. El demandado hacía entrevistas a personas para cubrir puestos de trabajo, pero realmente lo que hacía era robar su información personal para crear puestos ficticios para poder justificar el gasto por salarios de la empresa. Posteriormente el demandado se quedaba con las tarjetas prepagas a través de las que se pagaban los salarios de los trabajadores ficticios. En tres años consiguió un monto de USD 200.000.

Fuente: Estados Unidos

**Caso 10.** Lavado de ganancias provenientes del robo de identidad (2006).

Un acusado que dirigía un programa de tarjetas prepagas fue condenado por usar su programa para llevar a cabo el lavado de ganancias ilícitas para ladrones de identidad. Los ladrones crearon 21 cuentas de tarjetas con la información de identidad robada de las cuentas de los usuarios del proveedor de servicios de pago por Internet, y las cargaron con aproximadamente un millón de dólares estadounidense que posteriormente fue retirado a través de cajeros automáticos en Rusia.

Fuente: Estados Unidos

**Caso 11.** Fraude y lavado de dinero (2009).

Tres individuos fueron acusados de robar 5 millones de dólares al piratear la base de datos de una compañía de tarjetas prepagas, robar la información y manipular los saldos de las cuentas y los límites de las transacciones. Los acusados utilizaban la información de las tarjetas para crear duplicados de las mismas que utilizaban para retirar dinero de los cajeros automáticos en todo el mundo.

Fuente: Estados Unidos

### B) Servicios de Pago por Internet

**Caso 12.** Ardid fraudulento y lavado de dinero realizados mediante servicios de pago por Internet.

Con el objetivo de estafar a los compradores de libros de texto de un sitio Web comercial, un individuo creó aproximadamente 384 cuentas bancarias falsas destinadas a empleados inexistentes que se dedicarían a la venta de libros de texto. El individuo luego utilizó la información de las cuentas bancarias para abrir aproximadamente 568 cuentas de vendedores del sitio Web comercial empleando servicios de pago electrónico de persona a persona. El estafador anunciaba la venta de los libros de texto en todas las cuentas de los vendedores falsos del sitio Web llegando a recibir más de 5.3 millones de dólares. Posteriormente, el estafador transfirió las ganancias ilícitas desde las cuentas del servicio de pago por Internet de los vendedores hacia varias cuentas bancarias con sede en Singapur.

Fuente: Singapur

**Caso 13.** Fondos robados de cuentas bancarias blanqueados a través de cuentas de servicios de pago por Internet.

Un delincuente informático robó los datos personales que la víctima usaba para operar con la banca electrónica y luego abrió una cuenta fraudulenta en un proveedor de servicios de pago por Internet a nombre de la víctima, con datos personales falsos.

El delincuente designó una cuenta bancaria de referencia para suministrar a la cuenta fraudulenta de provisión de servicios de pago por Internet. Esta cuenta de referencia era la de la víctima. El delincuente realizó transferencias de la cuenta de referencia a la fraudulenta y posteriormente realizó transferencias de esa cuenta fraudulenta a otras cuentas dentro del mismo proveedor de servicios de pago por Internet. Las autoridades del orden no pudieron localizar los flujos de dinero ni descubrir la identidad del delincuente.

Fuente: Alemania

## *4.3 TIPOLOGÍA 3: Complicidad de proveedores de NMPs o de sus empleados*

### A) Tarjetas Prepagas

**Caso 14.** Sospecha del uso de tarjetas prepagas de circuito abierto y de sistemas de pago virtual para llevar a cabo el lavado de ganancias provenientes de la venta de droga.

Varios individuos fueron acusados de lavar sumas millonarias de dinero provenientes de la venta de estupefacientes a través de una compañía proveedora de tarjetas prepagas de circuito abierto. Los fondos fruto de la venta de drogas eran cargados en tarjetas prepagas y trasladadas al país de origen de la droga.

Estos individuos tenían cuentas en distintos países donde recibían fondos provenientes de diversos individuos y entidades dispersados geográficamente por América Central, Europa,

el Caribe, África, Asia, Asia del Sur y Canadá. Posteriormente, transferían el dinero a las cuentas donde se encontraba la compañía proveedora de tarjetas.

Además, se descubrió que dos proveedores canadienses de sistemas de pago por Internet enviaban dinero a la misma compañía de tarjetas prepagas. Ambos proveedores de sistemas de pago por Internet ofrecían el servicio de tarjetas prepagas a sus clientes, el cual era suministrado por la compañía facilitadora. Uno de los proveedores de sistema de pago por Internet era sospechoso de haber usado las tarjetas para blanquear el dinero de sus clientes provenientes del uso de esquemas Ponzi.[17]

Tipología adicional: Aporte de fondos por parte de terceros

Fuente: Canadá

### B) Servicios de Pago por Internet

**Caso 15.** Lavado de fondos ilícitos mediante el uso de moneda digital y tarjetas prepagas.

Una banda internacional de delincuentes transfirió dinero obtenido ilegalmente a través de un proveedor de servicios financieros a países de Europa del Este, donde era posteriormente retirado por miembros de la banda y convertidos en moneda electrónica con la participación de agentes de cambio de moneda digital. Esta moneda digital era posteriormente transferida a cuentas que mantenían los delincuentes con un proveedor de servicios financieros que manejaba moneda electrónica en los países involucrados. En cooperación con un banco ubicado en una zona extraterritorial, el proveedor de servicios financieros emitía tarjetas prepagas que podían ser adquiridas de forma anónima y utilizadas en la redes globales de cajeros automáticos.

Fuente: Alemania

[17] Según la Comisión de Cambio y Seguros de los Estados Unidos, el Sistema Ponzi es un fraude de inversión que consiste en el pago de beneficios a previos inversores mediante la inversión de nuevos inversores adheridos al esquema.

## CAPÍTULO 5: INCLUSIÓN FINANCIERA

Los avances tecnológicos asociados a los nuevos métodos de pago han demostrado que la inclusión financiera es una realidad. Los proveedores de servicios han visto el potencial de poder acceder al nicho escasamente explotado de los no bancarizados.

De los tres métodos de pago en este informe descritos, es el de servicios de pago móvil el que a vista de todos presenta más potencial de uso a medio y largo plazo. Las cifras son indiscutibles; hay países con más teléfonos celulares que personas. En países como Kenia o Filipinas el uso de los servicios de pago móvil se han convertido en operaciones regulares evitando que las personas se tengan que desplazar grandes distancias para realizar pagos, transferencias, o cualquier otra operación.

Las tarjetas prepagas, junto a los servicios de pago móvil, se consideran una buena herramienta de inclusión financiera. Aunque no llegan a los niveles de inclusión de los teléfonos celulares, ofrecen las mismas ventajas e incluso más variedad de operaciones. Sin embargo, según las características del servicio, comprenden también muchos más riesgos de LA/FT.

Los servicios de pago por Internet no son comparables con los dos métodos de pago anteriores. Tener Internet supone un lujo, especialmente en los países pobres o en desarrollo. Se puede decir que funciona como una medida de inclusión financiera en los países desarrollados donde el acceso a Internet está más a la orden del día.

Desde hace mucho tiempo, la inclusión financiera ha sido de gran interés para las organizaciones que promueven el desarrollo. En este contexto, el G-20 aprobó en la Cumbre de Seúl en 2010 el "Plan de Acción para la Inclusión Financiera".[18] En línea con la propuesta del G-20, el GAFI comenzó el diseño de una guía en 2011 para proporcionar apoyo en el diseño de medidas AML/CFT que faciliten los objetivos nacionales de inclusión financiera sin comprometer las medidas existentes para combatir el crimen. En febrero de 2013, el GAFI presentó el texto final de la guía donde desarrolla un conjunto de medidas AML/CFT exhaustivas y equilibradas para apoyar a las autoridades competentes y promover un entendimiento común de los estándares relevantes a la hora de promocionar la inclusión financiera y la flexibilización de los requerimientos, prestando especialmente atención al enfoque basado en el riesgo que permite a los países ajustar sus medidas de control acorde a los riesgos del producto o servicio.[19]

Si bien esta guía no se centra exclusivamente en los NMPs, sí menciona que éstos promueven la inclusión financiera de los sectores no bancarizados puesto que son accesibles, económicos y cubren las necesidades financieras fundamentales.

[18] G20, *Multi-Year Action Plan on Development*, Seoul, Noviembre 2010. http://www.g20.utoronto.ca/2010/g20seoul-development.html#inclusion
[19] FATF Report, Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, París, Febrero 2013. http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

En definitiva, la inclusión financiera y los controles ALA/CFT deben entenderse como complementarios. Se debe buscar un balance razonable entre ambos. De lo contrario, o tendríamos riesgos altos de LA/FT en algunos productos o servicios demasiado permisivos,

o nos encontraríamos con productos y servicios que dejan de ser atractivos tanto para los clientes como para el sector privado que los proporciona.

## CAPÍTULO 6: SITUACIÓN EN LA REGIÓN

Dentro de las actividades que contempla el Proyecto GAFISUD – Unión Europea. "*Apoyo a la lucha contra el lavado de activos en los países de América Latina y el Caribe",* relacionadas con el diagnóstico de la situación del Sector Financiero no Bancario, se encuentran el análisis del subsector de los "Nuevos Métodos de Pago" aprobado por el XXII Pleno de Representantes de diciembre de 2010.

Con el objetivo de poder hacer un diagnóstico de un subsector todavía poco desarrollado en la región y con el fin de entender mejor los riesgos que conllevan para poder eventualmente tomar una línea de acción común, se solicitó información sobre la situación nacional a las autoridades competentes de los países miembros. La información aportada ha sido esclarecedora y nos ha ayudado a entender la situación de un sub-sector en una región tan heterogénea en términos de avances tecnológicos, desarrollo económico y demanda de nuevos servicios.

Si hubiera que destacar un rasgo común en todos los países con respecto a los métodos de pago sería la marcada dependencia que aún existe de los pagos en efectivo. Aún así, se observa una ligera tendencia a la disminución de los medios de pago en papel y una evolución cada vez mayor hacia métodos de pago más modernos.

En líneas generales los países conocen los servicios y productos básicos ofrecidos por los NMPs. No obstante, se percibe una gran desinformación acerca de las características y funcionamiento del gran abanico de servicios y productos que realmente se encuentran ya disponibles en el mercado. Esta desinformación va acompañada del desconocimiento de una gran variedad de riesgos que aún no se están tomando en cuenta para prevenir el LA/FT.

A excepción de contados países, la mayoría carece de regulación específica para los NMPs. Algunos ya están discutiendo proyectos de regulación, otros ya las tienen pero no las acaban de implementar. En muchos países algunos NMPs quedan de algún modo controlados porque son proporcionados por entidades financieras bancarias y están sujetos a controles LA/FT, pero al mismo tiempo, las entidades financieras no bancarias que podrían también ofrecer estos productos y servicios quedan en el aire.

La región precisa identificar y evaluar profundamente los riesgos de estos servicios y productos para poder prevenirlos en el futuro. Que el mercado esté aún por desarrollar, no debe ser visto como un impedimento para tomar medidas, sino todo lo contrario; es una ventaja para las jurisdicciones poder entender la actualidad de los mercados de servicios de pagos y de este modo adelantarse a la aparición del problema.

La mayor parte de la población latinoamericana con rentas medias o bajas carece de acceso a servicios financieros a través de canales formales. A este hecho hay que sumarle que la baja competencia entre entidades financieras y los altos márgenes de intermediación encarecen la oferta financiera hasta tal punto de hacer inviable la prestación de servicios a ese nicho de población. Si bien es preciso no ignorar que la existencia de agentes o corresponsales no bancarios han contribuido a disminuir el umbral de la población desatendida, aún existe un alto porcentaje de la población que usa un sistema basado en el

dinero en efectivo. Este alto porcentaje representa un nicho de mercado con mucho potencial, que junto al crecimiento lento, aunque sostenido, de los NMPs en el continente hace prever un avance importante en el uso de esta tecnología como un método de inclusión financiera alternativa a los sistemas tradicionales.[20]

América Latina presenta una situación prometedora en el sector de los NMPs. Se percibe una alta penetración y una gran iniciativa por parte del sector privado que busca satisfacer nichos de demandas. También, el papel de los gobiernos ha demostrado ser fundamental para incentivar y educar en el uso de estos métodos a esa parte de la población no bancarizada. Varios países han puesto en prácticas iniciativas a gran escala para transferir subvenciones y ayudas a sus beneficiarios a través de medios electrónicos, al mismo tiempo que reducen costes de gestión y administración, y manteniendo además mayor control de la distribución y menos posibilidades de malversación de fondos.

Un dato que confirma el futuro prometedor de América Latina en este ámbito es que en la región el comercio electrónico está creciendo rápidamente. En este contexto, Brasil despunta en la región con ventas superiores a los 25 mil millones de dólares. Hay que indicar que la región no es homogénea y que cada país tiene una situación totalmente diferente a los demás. En el caso de Brasil, múltiples factores se han combinado para reflejar estos registros de ventas, como su desarrollo económico, la mejora de los índices de bancarización y de penetración de los medios de pago electrónicos, y mayor seguridad y confianza en el canal.[21]

Probablemente, de los tres métodos de pago descritos en este informe sean los servicios de pago móvil los que más éxito tendrán, permitiendo y facilitando la inclusión financiera de segmentos sub-atendidos o no atendidos por los métodos tradicionales. A pesar de ello, es difícil vaticinar el rumbo que tomará exactamente el mercado. Por el momento, la mayoría de los países de la región presentan una tasa alta de crecimiento del uso de la banca móvil. Estos servicios no son estrictamente servicios de pago, más bien son un canal intermediario entre el cliente y la entidad financiera, pero no hay que olvidar, que el incremento en el uso de este servicio proporcionará confianza a los usuarios y con el tiempo se puede esperar que demanden nuevos productos financieros como los métodos de pago móvil, entre muchos otros.

Se destacan en la región importantes iniciativas entre compañías de telefonía e instituciones financieras para ofrecer servicios de monedero móvil, como lo son Wanda que estará presente en 12 países y que es una iniciativa de Movistar y MasterCard; y Transfer del CitiGroup, América Móvil, Banamex e Inbursa. También en Perú, Scotiabank está trabajando en un monedero móvil.

Los gobiernos también están tomando iniciativas interesantes. En Colombia han desarrollado servicios a través del celular mediante los cuales los beneficiarios de subvenciones pueden recibir el importe en su teléfono móvil y sacar efectivo a través de cajeros asociados mediante un código y sin tarjeta.

---

[20] FOMIN, M-Banking, oportunidades y barreras para el desarrollo de servicios financieros a través de tecnologías móviles en América Latina y el Caribe, Banco Interamericano de Desarrollo, Nueva York, abril de 2009. P.8. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2011/02/Oportunitades.pdf

[21] Tecnocom, *Tendencias en Medios de Pago 2012*, Madrid, 2012. P. 12. http://www.afi.es/afi/libre/PDFS/Grupo/Documentos/Informe_Tecnocom12.pdf

Aún con todos estos avances, el pago móvil es un concepto muy nuevo y no hay mucha oferta en la región. Sin embargo, todo parece que la maquinaria para el éxito de estos servicios se está poniendo en marcha y se infiere que esta modalidad de pago ganará peso en el futuro.

Otro excelente método de pago para promover la inclusión financiera en la región son las tarjetas prepagas. Éstas ofrecen seguridad, practicidad y gran aceptación en el mercado, nacional, internacional y electrónico. Ayudan también a controlar los gastos, y a medio y largo plazo, promueven la educación financiera puesto que con el tiempo los no bancarizados tendrán mayor confianza en los servicios y podrán demandar nuevos productos. También complace a la globalización de la población activa que demanda métodos de envío de remesas más convenientes. Se estimó en 2012 que las remesas globales ese mismo año superarían los 400 mil millones.[22]

Las tarjetas prepagas, además, constituyen una tipología de producto muy versátil que puede ser usada por distintos tipos de consumidores, tanto bancarizados como no bancarizados satisfaciendo distintas necesidades. Por ejemplo, productos enfocados a jóvenes que disponen de bajos montos, que proporcionen mayor seguridad, y que posibiliten hacer pagos electrónicos; o para pagar dietas en el ámbito empresarial; o subvenciones por parte de los gobiernos.

A pesar de que el prepago representa aún una fracción muy pequeña dentro del mundo de las tarjetas, hay estimaciones que predicen que el mercado crecerá a un ritmo aproximado del 36%, y que las recargas mundiales en 2017 alcanzarán los 840 mil millones de dólares. Se estima que las recargas para América Latina variarán entre 81 y 160 mil millones.[23] Este panorama representa una oportunidad muy importante e interesante para todos los actores que puedan verse involucrados.

Ya se han tomado iniciativas en países de la región para promocionar tarjetas abiertas recargables, como por ejemplo en Perú, Chile, Brasil o México. En este último país, Visa y MasterCard han empezado recientemente a ofrecer servicios de envío de remesas desde EE.UU a México a las personas que cuenten con estas tarjetas. Es razonable que se hayan centrado en México teniendo en cuenta que es el primer país de América Latina receptor de remesas; según el Banco Mundial, México recibió en 2011 el equivalente al 2% de su PIB[24]. En Chile las tarjetas prepago se han utilizado en los programas de alimentación. Desde 2010, la Junta Nacional de Auxilio Escolar del Gobierno entrega las becas en formato electrónico sustituyendo al papel.[25]

Es importante destacar que la difusión del uso de la tarjeta prepaga promueve la inclusión financiera mientras se formalizan los flujos de capitales mediante canales regulares. Además, impacta positivamente en la vida de las personas, que con el tiempo serán susceptibles de demandar otros servicios financieros como seguros o créditos. Es

[22] Banco Mundial, Comunicado de prensa, *Países en desarrollo recibirán más de US$400.000 millones en remesas en 2012*, 20 de noviembre de 2012. http://www.bancomundial.org/es/news/press-release/2012/11/20/developing-countries-to-receive-over-400-billion-remittances-2012-world-bank-report
[23] Tecnocom, *Tendencias en Medios de Pago 2012*, Madrid, 2012. P. 53. http://www.afi.es/afi/libre/PDFS/Grupo/Documentos/Informe_Tecnocom12.pdf
[24] Banco Mundial, *Movilidad mundial no se ve afectada por la crisis financiera, como tampoco las remesas*. *Washington D.C.*, 2012. *http://goo.gl/T95Xy*
[25] Tecnocom, *Tendencias en Medios de Pago 2012*, Madrid, 2012. P. 65. http://www.afi.es/afi/libre/PDFS/Grupo/Documentos/Informe_Tecnocom12.pdf

improbable que las tarjetas prepagas sustituyan en su totalidad o desbanquen a las tarjetas de crédito/débito, sin embargo, sí que se presentan como una alternativa sólida para comprar por Internet o para segmentos de la población que requieren de mayor seguridad—como los jóvenes—ya que en caso de fraude o robo la cantidad sólo se limita al saldo de la tarjeta.

En el caso de Internet, aunque sus usuarios comienzan a expandirse en la región, aún queda un tramo muy largo para alcanzar los niveles de otras regiones geográficas. Esta realidad se refleja en el uso de servicios de pago por Internet. Si bien existen, éstos suelen estar relacionados especialmente con operaciones realizadas por medio de portales bancarios.

Uno de los sistemas no bancarios de servicios de pago por Internet líder en la región es DineroMovil. Opera en Argentina, Brasil, Chile y México. El sistema permite al cliente que desea efectuar pagos a través del portal hacer una depósito previo de una cantidad determinada a través de multitud de canales. Una vez hecho el depósito, el cliente puede hacer pagos en línea con comerciantes registrados y transferir dinero a otras personas. Si no se dispone de suficientes fondos en la cuenta se puede recargar más dinero o dejarlo en un estatus pendiente hasta que se recargue más dinero.

Los pagos por Internet más usuales usan empresas que llevan a cabo transacciones en Internet en las que los clientes pueden pagar a través de la red pero utilizando sus tarjetas de crédito/débito o cuenta bancaria. En este contexto, la empresa es tan sólo un canal intermediario entre el establecimiento comercial y el cliente del banco. Aún no se acaba de expandir el mantenimiento de una cuenta prepaga con el proveedor.

Todos los datos indican que el sector de los NMPs en la región experimentará un gran desarrollo en un futuro a corto y medio plazo. Son ilustrativos los ejemplos de Kenia y Filipinas donde una gran parte de la población hace uso habitual de estos métodos. Entender con detalle los riesgos de este subsector facilitará la labor de los países en la implementación de sus regulaciones de lucha contra el LA/FT. Los países deben aprovecharse del panorama de la región, pues presenta las condiciones más convenientes para adelantarse al problema e implementar una estrategia preventiva reactiva y dejar a un lado las estrategias pasivas enfocadas a combatir el problema una vez que ya ha aparecido.

# CAPITULO 7: EJEMPLOS ILUSTRATIVOS

## *7.1 Estudio 1: Pago Móvil en Filipinas*

### Panorama del Sector

Durante la última década el gobierno filipino ha priorizado en su agenda la inclusión financiera de la población con ingresos más bajos. Con estudios centrados en las características y dinámicas del mercado, el gobierno encontró oportunidades interesantes en nuevos modelos financieros como los servicios de pago móvil. Actualmente Filipinas puede presumir de haberse convertido en uno de los líderes mundiales en este sector.

Las demandas del mercado potenciaron el desarrollo de nuevos modelos que satisficiesen las necesidades del público, como por ejemplo la posibilidad de recibir remesas internacionales en el celular. Uno de cada diez filipinos vive en el exterior y regularmente envía remesas a su país. El promedio de envío es de 300 dólares lo cual tiene un coste de entre 7 y 33 dólares, o entre el 2,5 y 10% del valor enviado mediante los mecanismos tradicionales. Usando los servicios de pago móvil el coste se reduce al 1%.[26]

La penetración del celular en Filipinas es de más del 75%. El Banco Central de Filipinas, el Bangko Sentral ng Pilipinas (BSP) quiso explotar dicha cifra e implementó una aproximación muy interesante destinada a ofrecer nuevos servicios a aquella población financieramente ignorada. La estrategia del gobierno se centró en mantener continuas consultas y conversaciones con los operadores móviles interesados en desarrollar los servicios financieros móviles; de esta manera, se le permitió al sector privado que lanzase sus productos mientras que el BSP evaluaba los riesgos existentes para poder finalmente perfilar la regulación más apropiada.

Actualmente, son dos los operadores móviles que ofrecen el servicio de pago móvil. El pionero fue Smart Communications (Smart) que utiliza un esquema de cuenta prepagada en donde un banco terceriza una parte sustancial de sus actividades al operador móvil. En segundo lugar se encuentra el operador móvil Globe Telecom (Globe) que a través de su subsidiaria (G-Xchange Inc) ofrece una cuenta prepagada no bancaria a los clientes;

### Regulación

En su ímpetu por potenciar los servicios financieros a través del celular, el BSP flexibilizó su regulación mediante la **Circular 471** (2005) que permitió que los agentes de cambio y remesa correctamente registrados pudieran realizar muchas de las operaciones que hasta entonces sólo podían realizar las instituciones financieras, como por ejemplo, las operaciones de recepción y emisión de dinero en efectivo.[27]

Mediante esta circular, los agentes registrados quedan sujetos al **Acto de la República N° 9160** sobre la lucha contra el lavado de activos, y por lo tanto están obligados a llevar a

[26] CGAP, *Notes on Regulation of Branchless Banking in the Philippines*, 2010.
http://www.cgap.org/sites/default/files/CGAP-Regulation-of-Branchless-Banking-in-Philippines-Jan-2010.pdf
[27] Bangko Sentral ng Pilipinas, Circular No. 471, Series de 2005.
http://www.bsp.gov.ph/regulations/regulations.asp?id=116

cabo la apropiada identificación de clientes, el mantenimiento de registros y los reportes de operaciones sospechosas.[28] Además, los agentes han de recibir un curso de capacitación sobre la lucha contra el lavado de activos por el Consejo Anti-Lavado de Dinero del BSP.

La Sección 8 de la Circular 471 especifica las obligaciones de los agentes a la hora de aplicar medidas de Debida Diligencia del Cliente. Ante cualquier operación, los agentes deberán requerir y conservar la siguiente información:

- Fecha
- Nombre y firma del remitente
- Dirección postal actual
- Dirección postal permanente
- Fecha y lugar de nacimiento
- Número de teléfono
- Nacionalidad
- Moneda y monto de la transferencia que se solicita
- Fuente de la moneda extranjera
- Nombre y relación con lo/s beneficiario/s

Además de la lista anterior, los clientes deberán presentar los documentos de identidad reconocidos por el gobierno en los comercios habilitados para tramitar el alta de servicios.[29]

En la Sección 9 quedan definidos los requerimientos de los agentes en cuanto al reporte de operaciones sospechosas al Consejo Anti-Lavado de Dinero. Los reportes deberán ser enviados dentro de los cinco días hábiles desde que se efectuaron dichas transacciones o desde que el agente recibió la información de la transacción.

La puesta en funcionamiento de la Circular 471, ayudó en gran medida a que el BSP mantuviese un estricto control sobre los riesgos y debilidades de los productos de pago móvil al mismo tiempo que relajaba medidas para que permitiesen que los servicios financieros llegaran al máximo número de personas posible.

Tras varios años observando los productos de pago móvil del país, el BSP reguló la emisión de dinero electrónico mediante la **Circular 649** de 2009.[30] Dicha resolución reconoce tres posibles tipos de emisores de dinero electrónico:

- Bancos.
- Instituciones financieras no bancarias.
- Instituciones financieras no bancarias registradas con el BCP como agentes de transferencia de dinero.

[28] Gobierno de Filipinas, Acto de la República No. 9160, Julio 2001, (Enmendado por el Acto de la Republica N. 9194). http://www.gov.ph/2001/09/29/republic-act-no-9160/

[29] La Circular No. 564 de 2007 especifica los nuevos requerimientos de identificación válida para transacciones financieras. http://www.bsp.gov.ph/regulations/regulations.asp?id=1745

[30] Bangko Sentral ng Pilipinas, Circular No. 649, Series de 2009 http://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf

Para que estas entidades puedan ser reconocidas como emisores de dinero electrónico deben cumplir con ciertos requisitos previstos en los manuales de regulación para bancos y para instituciones financieras no bancarias.[31]

La Circular 649 define también los principales requerimientos para los emisores de dinero electrónico cuyo incumplimiento está sujeto a penalizaciones, entre ellos:

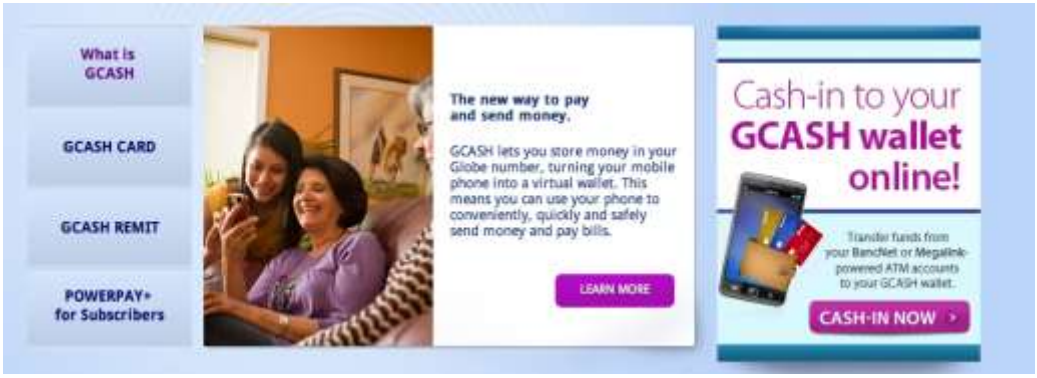
- Límite de valor mensual por cliente de PHP 100.000 (USD 2444,99) independientemente del número de productos de que disponga.
- Sistema de mantenimiento de registros tanto del dinero electrónico emitido, como de la identidad de los clientes y sus balances. Además, el sistema tiene que ser capaz de poder monitorear las transacciones y poder conectar directamente el dinero emitido con los clientes.
- El dinero electrónico debe tener un valor nominal invariable.
- El emisor de dinero electrónico debe asegurar que sus distribuidores o agentes cumplan con todos los requisitos de ALA/CFT.

**Productos de Pago Móvil**

***Smart Money***.[32] Este modelo utiliza un esquema de cuentas prepagas centradas en los bancos socios de Smart. Los bancos son los responsables de supervisar las operaciones y enviar las operaciones sospechosas al BSP. Smart Money ofrece dos plataforma, una de banca móvil y otra de e-money (monedero electrónico). La plataforma de banca móvil permite a los clientes realizar recargas, pagar facturas, transferir fondos a terceros que dispongan de una cuenta Smart, y multitud de otras transacciones que sólo podrían realizarse a través de un cajero automático. La plataforma de e-money tiene asociada una tarjeta recargable válida para cualquier ATM o banco asociado, y puede ser usada para hacer cualquier pago en aquellos lugares donde acepten Mastercard.


[31] Manual de Regulación para Bancos: http://www.bsp.gov.ph/downloads/Regulations/MORB.pdf
Manual de Regulación para Instituciones no Bancarias: http://www.bsp.gov.ph/downloads/regulations/mornbfi.pdf
[32] Smart, Smart Money, http://www1.smart.com.ph/money/what/#

***GCash***.[33] Esta modalidad permite a los clientes recargar con efectivo sus carteras electrónicas a través de las cuales pueden hacer pagos vía SMS a otros clientes GCash o pagar facturas. El valor de las cuentas e información de las transacciones son mantenidas por la subsidiaria de Globe (GXI) la cual está registrada como agente de remesas y mantiene cuentas conjuntas en distintos bancos.




***Características comunes de los productos:***

- Para darse de alta en el servicio, los clientes deben presentarse personalmente en los centros autorizados o ante los agentes de remisas registrados con su documento de identidad y cumplimentar debidamente una solicitud de alta.
- Los clientes están sujetos a estrictas medidas de DDC.
- Se mantienen registros por 5 años.
- Continuo monitoreo de transacciones sospechosas.
- Límites de valor:
    - Única transacción limitada a PHP 10.000 (aproximadamente USD 217).
    - Límite diario de PHP 40.000 (aproximadamente USD 866).
    - Límite mensual PHP 100,000 (aproximadamente USD 2.165).
- Permiten entrada y salida de dinero en efectivo a través de agentes.
- Permiten la recepción de remesas desde el extranjero; los límites vendrán determinados por el operador móvil que ofrece el servicio.
- Permiten recargar las cuentas por banca móvil, centros y agentes autorizados, cajeros automáticos y transferencia en línea.

## *7.2 Estudio 2: Tarjetas Prepagas en Australia*

Las tarjetas prepagas tienen una pequeña pero incipiente presencia en el mercado de pagos en Australia. Estas tarjetas toman formas que varían desde tarjetas recargables a no

[33] Globe GCash, http://gcash.globe.com.ph/

recargables, conectadas a una cuenta bancaria a nombre del cliente o sin una cuenta específica, limitadas al uso en ciertos comercios o abierta a un uso más amplio.

Es cierto que Australia a pesar de tener un gran potencial de uso comenzó la carrera hacia el uso de tarjetas prepagas un poco tarde. Este efecto se debe especialmente al monopolio de las grandes proveedoras de tarjetas de crédito/débito internacional. Aún así, Australia ha empezado a experimentar bastante éxito en un esquema de tarjeta destinada al turismo y que funciona como una buena alternativa para sustituir otros productos de viajes como cheques de viajero, tarjetas de crédito y/o débito. Además, estas tarjetas ofrecen incluso la posibilidad de contener distintos monederos cargados con divisas extranjeras, lo que hace mucho más fácil el control de capital a la hora de viajar puesto que el precio de la divisa se bloquea con el mismo precio que se introdujo en el monedero.

**Regulación**

En Australia las tarjetas prepagas son entendidas como un dispositivo portátil capaz de almacenar dinero en un formato distinto del físico. En lo que respecta el LA/FT, las tarjetas prepagas quedan reguladas mediante el *Anti-Money Laundering and Counter-Terorism Financing Act 2006*[34] que proporciona los medios para detectar y disuadir el lavado de activos, y el *Anti-Money Laundering and Counter-Terorism Financing Rules Instrument 2007*[35] que contiene los detalles sobre cómo deben ser llevadas a cabo las obligaciones apuntadas en la normativa de 2006.

La regulación australiana está compuesta de varios pilares obligatorios para los negocios regulados los cuales son entendidos como entidades reportantes de servicios designados. Entre los servicios designados se encuentran las tarjetas prepagas.

Las entidades reportantes estarán sujetas a las siguientes obligaciones bajo penalizaciones por incumplimiento:

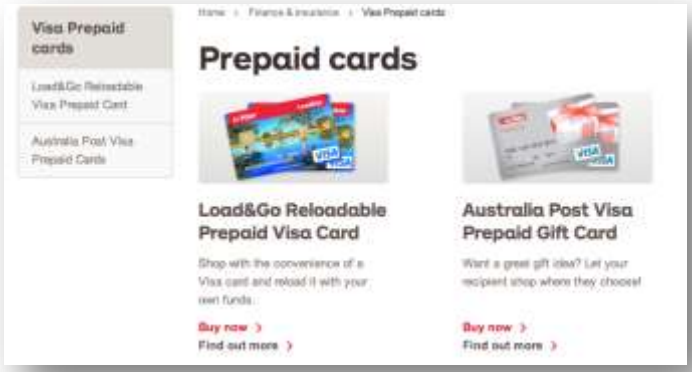
- **Registro**. Todo negocio regulado debe registrarse con el Centro de Análisis y Reporte de Transacciones de Australia (AUSTRAC, por sus siglas en inglés). Para poder registrarse deben proporcionar información sobre el negocio y los servicios que provee, además de mantener un registro actualizado de sus datos, de sus negocios y de su actividad financiera anual. AML/CFT Act, Parte 6.
- **Identificación del cliente.** La entidad reportante deberá asegurar que recoge como mínimo el nombre completo, la fecha de nacimiento y la dirección del cliente. Además, la entidad reportante deberá verificar dichos datos mediante documentación fiable. AML Rules, Capítulo 4.
- **Mantenimiento de registros.** Las entidades reportantes deberán mantener registro de los servicios designados que proporcionan, de cualquier dato de identificación del cliente, copia de documento, del programa AML/CFT y de las transacciones por un período de 7 años. AML/CFT Act, Parte 10.
-

[34] Gobierno de Australia, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.* http://www.comlaw.gov.au/Details/C2006A00169
[35] Gobierno de Australia, *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007.* http://www.comlaw.gov.au/Details/F2007L01000

- **Implementación de programas de AML/CFT.** Las entidades reportantes deberán implementar programas AML/CFT que establezcan controles o sistemas basado en el riesgo apropiados de manera que las entidades puedan identificar, administrar y mitigar riesgos de LA/FT de servicios designados, metodología o tecnología antes de que sean adoptados o sean lanzados al mercado. AML Rules, Capítulo 8.
- **Debida Diligencia del Cliente continua.** Las entidades reportantes deberán implementar sistemas y controles basados en el riego para determinar si se debe solicitar más información al cliente en los casos en que se requiera, así como un programa de monitoreo de las transacciones sospechosas realizada por los clientes. AML Rules, Capítulo 15.
- **Reporte de actividad sospechosa.** La entidad reportante está sujeta a la obligación de reportar a AUSTRAC asuntos sospechosos, como por ejemplo las transacciones de 10.000 dólares australianos o más, así como aquellos casos en los que una persona envíe o reciba una transferencia internacional de fondos. Del mismo modo, AUSTRAC puede requerir a las entidades reportantes que envíen reportes de cumplimiento de AML/CFT. AML/CFT ACT 2006, Parte 3, División 2.
- **Transferencias.** Las transferencias electrónicas quedan registradas con información del que la realiza y del beneficiario. AML/CFT ACT 2006, Parte 5. También las transacciones mediante dinero en efectivo realizadas a través de agentes deben quedar registradas. Esta obligación queda enmarcada dentro del *Financial Transaction Report Act 1988*.[36]
- **Debida Diligencia de Empleados.** Las entidades reportantes deberán implementar un programa de debida diligencia de sus empleados para identificar a aquellos que estén en una posición de facilitar la comisión de delitos de lavado de dinero o financiación del terrorismo en conexión con la provisión del servicio designado que ofrece. AML Rules, Capítulo 8.

**Producto de Tarjeta Prepaga**

**Australian Post Load&Go Travel Card.**[37] Se trata de una tarjeta prepaga Visa que puede ser usada en cualquier parte del mundo para retirar dinero en efectivo desde cualquier cajero automático que opere con Visa y para realizar compras de productos y servicios en tiendas, en línea o por teléfono donde Visa sea aceptada electrónicamente.




La tarjeta puede ser recargada con un máximo de

[36] Gobierno de Australia, *Financiar Transaction Report Act 1988.* http://www.comlaw.gov.au/Details/C2013C00009
[37] Australian Post, Load&Go Reloadable Prepaid Visa Card. http://auspost.com.au/finance-insurance/load-and-go-travel-card.html

10.000 dólares australianos y dicha cantidad puede mantenerse en cinco divisas distintas: dólares australianos, dólares neozelandeses, dólares norteamericanos, euros o libras esterlinas. La cantidad mantenida en cada divisa está separada en distintos monederos. Se puede transferir dinero de un monedero a otro una vez el cliente se ha registrado como el dueño de la tarjeta en la página web de la tarjeta. Cuando se transfiere de un monedero a otro se tomará la tasa de cambio de divisa que esté establecida en el momento por Australian Post.

La tarjeta tiene varios límites:

- Sólo se permite una tarjeta por persona.
- Sólo ciudadanos australianos pueden adquirirla.
- Se necesita una recarga mínima de AUD 100.
- Se establece una recarga máxima de AUD 10.000.
- El balance máximo disponible no superará los AUD 10.000.
- La recarga máxima agregada en un período de 12 meses será de AUD 25.000.
- La extracción máxima en efectivo desde un cajero automático será de AUD 2.500.
- Todas las recargas que se hacen en la tarjeta deben hacerse en dólares australianos.

Este programa de tarjeta ha establecido un plan de funcionamiento que lleva a la tarjeta a funcionar como un producto con un menor riesgo. Los límites de valor establecidos para estas tarjetas corresponden con la naturaleza de un producto pensado para el turismo y el consumo.

Aunque el registro se pueda hacer por Internet, la tarjeta debe ser adquirida en un local de venta al público de Australian Post donde se deberá cumplimentar una solicitud y posteriormente pasar un proceso de verificación de la identificación del comprador.

Una vez adquirida la tarjeta, el cliente debe registrarse en la página web aportando nombre, dirección, email y fecha de nacimiento para autentificarse como el dueño de la tarjeta lo que servirá para poder hacer los controles de seguridad necesarios, así como el mantenimiento de registro correspondiente.

La tarjeta puede ser recargada bien en el local de venta de Australian Post, a través de la página postbillpay.com.au, o vía “Pay Anyone” que es un método de pago que muchos bancos y otras instituciones financieras ofrecen. En cualquier caso el cliente debe proporcionar información personal por lo que siempre queda un registro que permite satisfacer controles de seguridad.

### *7.3 Estudio 3: Esquema de Moneda Virtual. Bitcoin*

El caso de Bitcoin es sin duda particular. No se trata de un método de pago por Internet de forma estricta, sino que representa un esquema de moneda virtual que opera a nivel mundial basado en una red de pares descentralizada (también conocida por su denominación en inglés como *peer-to-peer*) y que se ha convertido por el momento en el más exitoso y controvertido entre todos los esquemas virtuales existentes. Al igual que

cualquier otra moneda oficial, el Bitcoin permite todo tipo de transacciones, ya sean transferencias a otras personas o compras de productos de forma anónima.

El Bitcoin no se ajusta a las dinámicas de funcionamiento de ninguna moneda oficial, sino que su valor queda definido según la demanda de la misma en el mercado. Al tratarse de una red de pares descentralizada, Bitcoin no depende de una cámara central de compensación y ninguna otra institución está involucrada en la transacción. Son los usuarios de esta moneda virtual los que quedan a cargo de cualquier operación que normalmente realizarían las instituciones financieras tradicionales. No existe ninguna autoridad central que se encargue del control del suministro de dinero sino que tal suministro dependerá de los recursos—electricidad y tiempo de CPU—que los usuarios conocidos como "mineros" dedican a solventar problemas matemáticos específicos.

Los clientes que quieran adquirir Bitcoins lo podrán hacer a través de plataformas de cambio de moneda virtual donde los compradores realizan operaciones de compra y venta. El precio de la moneda dependerá de su valor actual al que probablemente hay que sumar un impuesto de cargo de operación para la plataforma de cambio. Para poder almacenar y usar Bitcoins, los usuarios deberán descargarse e instalar un software gratuito en su computadora donde podrán almacenar en un monedero virtual sus Bitcoins. Se recomienda además que los usuarios tengan las medidas de seguridad adecuadas instaladas en sus computadoras porque en caso de que un pirata informático tenga de algún modo acceso a la computadora, y especialmente al archivo que contiene los Bitcoins, éstos puedes ser sustraídos y no habrá manera de recuperarlos.

Las características de Bitcoin lo convierten en un producto altamente atractivo, no sólo para un público que quiere mantener su dinero fuera de cualquier institución financiera, sino también para criminales que buscan siempre nuevas formas de mantener el fruto de sus operaciones de forma segura. Por un lado, las transacciones son totalmente anónimas; no existen cuentas bancarias sino que las cantidades de Bitcoins pasan de una computadora a otra. Por otro lado, las transacciones se realizan mucho más rápido y son también más baratas que en los métodos de pago tradicionales. Si hubiese algún impuesto, éste suele ser muy bajo y por supuesto no hay impuesto por uso o tenencia de una cuenta bancaria.

**Novedades**

Junto con Bitcoin han aparecido además nuevos productos que lo complementan. Uno de estos productos es Bitbills.[38] Consiste en una tarjeta prepaga para almacenar Bitcoins y puede servir para hacer transacciones de pago en un establecimiento de venta. Cada Bitbill contiene un holograma de seguridad especial que contiene un código QR que a su vez codifica una clave criptográfica de un solo uso privado y que representa el dinero

[38] Bitbills, http://bitbills.com/

almacenado en la tarjeta. Los clientes pueden cambiar el importe a valor nominal (vendiéndola en un minorista), o bien introducir el importe en la red Bitcoin una vez extraída la clave privada de la tarjeta.


La expansión de los Bitcoins no se limita sólo al mundo virtual. Recientemente una empresa ha confirmado la producción de cajeros automáticos llamados BitcoinATM que permitirán adquirir la moneda digital o cambiarla por efectivo sin necesidad de hacer una transacción a través del celular o de la computadora.

Hasta hace poco existía otro producto interesante llamado Bitcoin 2 Credit Card, que era una tarjeta de crédito virtual ofrecida a cambio de Bitcoins. Los compradores de estas tarjetas virtuales recibían los datos necesarios de la tarjeta virtual para poder realizar cualquier tipo de transacción en línea. A pesar de que no esté en funcionamiento nos muestra la amplia gama de opciones que irán apareciendo para el Bitcoin.

**Funcionamiento**

Según el fundador de Bitcoin, Satoshi Nakamoto,[39] un Bitcoin se define como una cadena de firmas digitales. Todo aquel que posea la moneda tendrá un par de claves, una pública y otra privada, que son almacenadas en un archivo en la computadora.

Para iniciar una transacción el futuro dueño de la moneda tendrá primero que enviar su llave pública al dueño original de la moneda. El dueño original tendrá que firmar digitalmente la transacción previa con el resultado de un algoritmo determinado (hash en inglés)[40] y también la llave pública del futuro dueño. Toda transacción queda registrada en el código de la moneda por lo que sólo el nuevo dueño será el único posible usuario; la moneda tendrá un solo uso, y al usarla de nuevo se añadirán nuevos códigos que la diferenciarán de la anterior.

Utilizando una explicación más sencilla e ilustrativa se podría parangonar los Bitcoins con un tipo de "Email especial" que no puede ser copiado, y que cuando se envía a otra persona, el Email se borra automáticamente de la casilla de correo electrónico donde estaba originalmente y pasa a estar en la casilla del destinatario. Otro modo sería imaginarse a un grupo de individuos alrededor de una mesa. Cada individuo tiene una computadora con acceso en tiempo real a un registro contable que da cuenta del número de Bitcoins que cada uno posee en cada momento. El saldo de Bitcoins de cada individuo es una información

[39] El nombre Satoshi Nakamoto es un nombre ficticio. Actualmente se desconoce quién es exactamente el fundador de esta moneda.
[40] Un hash es el resultado de operaciones matemáticas muy complejas, que son fáciles de reproducir pero imposibles de revertir y difíciles de predecir.

pública y cada individuo que quiera hacer una transacción a otro tendrá que anunciárselo a todos los que están sentados en la mesa. Una vez anunciada la transacción, todo el grupo la añade al registro por lo que es necesario que todos los individuos verifiquen la autenticidad de dicha transacción. En un sistema como este, un individuo no puede gastar más de una vez una misma moneda porque en caso de que lo intentase la operación sería detectada y rechazada por todos los demás.[41]

En el mundo real de Bitcoin, los participantes están distribuidos en una red de pares global, y toda las transacciones tienen lugar entre direcciones en lugar de individuos. La posesión de estas direcciones es verificada mediante criptografía, sin revelar quiénes son sus respectivos dueños. Los sistemas que validan las transacciones son conocidos como "mineros" y se tratan de computadoras muy potentes conectadas en la red de Bitcoin que realizan cálculos matemáticos complejos que persiguen verificar la validez de las transacciones. Las personas que usan estos sistemas lo hacen de forma voluntaria pero reciben una cantidad de Bitcoins cada vez que su sistema encuentra una solución. Es importante destacar que la única manera de introducir nuevos Bitcoins en el sistema es a través de las recompensas por el trabajo de los mineros. Una vez creadas, estas monedas pueden ser vendidas y compradas en el mercado en línea.

Según Bitcoin, el esquema ha sido técnicamente diseñado para que la provisión de moneda siga un curso predecible con un número finito de 21 millones de monedas que será alcanzado en 2040.


**Fuente: Bitcoin**

A medida que se acerca esa fecha, los algoritmos que tienen que ser resueltos por los mineros serán cada vez más y más complejos. A partir de 2040, los mineros se financiarán mediante impuestos de transacción porque ya no podrán ser recompensados con unidades de monedas.

## Riesgos

[41] Morgan E. Peck, "The Cryptoanarchists' Answer to Cash," *IEEE Spectrum*, Junio 2012. http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/2

Los riesgos que comportan las monedas virtuales no difieren de los riesgos que comporta el dinero en efectivo: lavado de activo, financiación del terrorismo, tráfico de estupefacientes, evasión fiscal, etc.

Muchos identifican el sistema Bitcoin como un sistema de Ponzi. Los usuarios entran en el sistema comprando Bitcoins pero sólo pueden canjearlos en dinero real si otros usuarios quieren comprar sus Bitcoins, por lo que nuevos usuarios tendrán que ir entrando en el sistema.

En los últimos años los medios de comunicación han informado de eventos que alertan de los riesgos de Bitcoin. En 2011, un ciber ataque hizo que la moneda que cotizaba entonces a USD 17.50 bajase hasta 0.01 en apenas unos minutos. Unos 400.000 Bitcoins—un valor aproximado de 9 millones de dólares—se vieron afectados. Una cuenta con muchas Bitcoins fue robada y sus monedas fueron vendidas y compradas automáticamente después con el objetivo de sacar su valor en efectivo. Afortunadamente, dicha cuenta había establecido un límite de extracción diario de 1000 dólares por lo tanto el ladrón no se pudo llevar una cantidad mayor a aquella cifra. Además, el ladrón tuvo acceso a los datos de la plataforma de cambio MT. Gox y pudo robar nombres de usuarios, Emails y contraseñas de miles de usuarios. MT. Gox pudo actuar cerrando el sistema durante varios días hasta que solventó el incidente.[42]

Otro evento relacionado con la seguridad del sistema ocurrió en 2012. La plataforma de cambio Bitcoinica perdió más de 18.500 Bitcoins de su depósito tras un ataque cibernético robando probablemente también información sensible de clientes.

**Regulación**

Desde el punto de vista normativo, los esquemas de moneda virtual no se encuentran regulados y dejan lugar a actividades ilícitas.

A pesar de que en la **Unión Europea** existen regulaciones como la Directiva sobre el Dinero Electrónico (2009/110/EC) y la Directiva sobre Servicios de Pago (2007/64/EC) en ninguna de las dos queda enmarcado el Bitcoin.

En la Directiva sobre el Dinero Electrónico se utilizan tres criterios para definir el dinero electrónico: 1) debe ser almacenado electrónicamente, 2) emitido una vez recibidos los fondos de una cantidad no menor al valor monetario emitido, 3) aceptada como medio de pago por empresas que no sean el mismo emisor.

En principio el Bitcoin cumple con la 1) y la 3) pero no con la 2). Mediante los "mineros" se producen monedas pero éstas no son el producto de un intercambio de valor monetario

previo sino que se trata del fruto del trabajo aportado por los mineros. Además el Art.11 de la Directiva dice que "l*os Estados Miembros velarán por que los emisores de dinero electrónico reembolsen al titular del mismo, cuando éste así lo solicite, en todo momento y*

[42] Comunicado de prensa, MT. Gox, Marzo 2011. https://mtgox.com/press_release_20110630.html

*por su valor nominal, el valor monetario del dinero electrónico de que se disponga*"[43], y esto no puede ser asegurado en un esquema de moneda virtual como el Bitcoin.

En el caso de la Directiva sobre Servicios de Pago se establece la regulación sobre la ejecución de transacciones de pago cuyos fondos están compuestos por dinero electrónico pero no regula la emisión de dinero electrónico. Por lo tanto, la nueva categoría de proveedor de servicios de pago que introduce, a saber, instituciones de pago, no debería poder emitir dinero electrónico, y como consecuencia el Bitcoin quedaría fuera de esta normativa.

En los **Estados Unidos**, la Red contra los Delitos Financiero (FinCen, por sus siglas en inglés) del Departamento del Tesoro, presa de la importancia que las monedas virtuales están adquiriendo, emitió el pasado 15 de marzo una guía interpretativa sobre la aplicación de la normativa antilavado de las monedas virtuales.[44] Es objetivo principal de los Estados Unidos prevenir el alto riesgo que este nuevo producto conlleva ya que facilita la colocación, integración y disimulo del dinero proveniente de actividades ilegales.

El FinCen aclara que los intercambiadores de moneda virtual son considerados como remeseros de dinero (o Money Service Business en inglés) y que por lo tanto deben quedar registrados con el FinCen y estar sujetos a la regulación pertinente. No obstante, es importante destacar que aquellas personas que usan la moneda sólo para transacciones personales, como recibir pagos por servicios personales o para comprar bienes en línea no estarán afectados por la guía, por lo que de igual modo deja muchas lagunas legales que pueden ser explotadas por criminales.

De nuevo se aprecia en este caso que la tecnología y la innovación se adelanta a las normativas. Debería ser imperativo mantener una alerta especial a los riesgos que estos avances puedan crear e cuanto al LA/FT. Es necesario profundizar y realizar un análisis más exhaustivo de los esquemas de moneda virtual partiendo de la base de que probablemente los criminales ya los utilizan.

En **Canadá**, al igual que en el resto de jurisdicciones, los Bitcoins no están regulados en lo que respecta al control y supervisión. Sin embargo, recientemente el Servicios de Ingresos Públicos de Canadá anunció que toda transacción comercial en la que se utilice Bitcoins—incluso cuando se trate de un trueque o permuta—deberán ser tasadas de acuerdo a la normativa fiscal dispuesta en el Boletín IT-490.[45] Los Bitcoins pierden con esta regulación su principal atractivo, es decir, el no tener que pagar ningún impuesto.

## CAPÍTULO 8: CONCLUSIONES

El mercado de los NMPs ha experimentado un crecimiento considerable a nivel mundial

[43] Parlamento Europeo y Consejo de Europa, Directiva 2009/110/CE, Artículo 11. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:01:ES:HTML
[44] Red contra los Delitos Financieros, Guía sobre Monedas Virtuales y Responsabilidades Regulatorias, http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf
[45] Servicios de Ingresos Públicos, Boletín IT-490, http://www.cra-arc.gc.ca/E/pub/tp/it490/it490-e.txt

durante la última década y las previsiones a corto y medio plazo auguran un desarrollo más pronunciado. Las demandas del mercado han definido la evolución de los NMPs agudizando la tendencia del paso del papel al formato electrónico, en un mundo cada vez más globalizado y digitalizado. Los nuevos productos se ajustan a las necesidades de los consumidores que buscan productos más seguros, económicos, accesibles y rápidos **(Capítulo 2)**.

Al igual que cualquier otro sistema de pago, los NMPs han demostrado no estar exentos de riesgos de abuso para actividades de LA/FT. Las nuevas tecnologías y las lagunas regulatorias se han convertido en el mejor instrumento para los criminales especialistas en encontrar fallas en los sistemas para explotarlos como ilustran las tipologías descritas en el presente informe **(Capítulo 4)**.

El análisis llevado a cabo en este informe, junto a los resultados descritos en previas publicaciones del GAFI, ha sido fundamental para identificar multitud de riesgos que evidencian la falta de control y supervisión de los nuevos productos y servicios de estas alternativas de pago. Asimismo, se ha podido demostrar que las 40 Recomendaciones del GAFI aprobadas en febrero de 2012 proporcionan el marco regulatorio apropiado para minimizar las amenazas de LA/FT a sus niveles más bajo **(Capítulo 3)**.

La aplicación de un enfoque basado en el riesgo permite que los requerimientos de control y supervisión, así como otras medidas mitigadoras, puedan ajustarse a los nuevos productos y servicios, permitiendo no sólo reducir los riesgos de LA/FT, sino también promoviendo la inclusión financiera mediante NMPs viables con requisitos de control y supervisión razonables **(Capítulo 5 y 7)**.

En este contexto, Latinoamérica se encuentra en el punto de mira ya que parece reunir todas las condiciones para experimentar un gran desarrollo del sector. Algunos países ya han dado los primeros pasos para normalizar estas alternativas de pago aunque existe un generalizado desconocimiento de las características, funcionamiento, y amenazas de estos servicios debido al poco desarrollo del mercado en la región. Se estima que la situación actual es propicia para que los países se adelanten al los problemas e implementen estrategias preventivas reactivas que sirvan para reducir riesgos en las fases de diseño de los productos **(Capítulo 6)**.