BETTER THAN CASH ALLIANCE

PRÁCTICAS E INFORMACIÓN GENERAL

JULIO DE 2016

8 buenas prácticas para pagos digitales responsables

8 BUENAS PRÁCTICAS PARA PAGOS DIGITALES RESPONSABLES

Nota: Este documento fue ligeramente revisado en junio 2017.

Para que los clientes adopten y usen los pagos digitales, deben sentirse tratados de manera justa y protegidos frente a riesgos tales como la pérdida de privacidad, la exposición al fraude y las cuotas no autorizadas. Por ese motivo, los proveedores de servicios deben procurar activamente tomar medidas para proteger a sus clientes y que los reguladores garanticen un marco regulatorio sólido de protección al consumidor. Esto es particularmente importante para los clientes que sufren exclusión y marginación financiera, en especial para las mujeres y para aquellos con baja capacidad financiera y tecnológica, que se manejan en un mundo de rápida innovación con nuevos tipos de servicios, proveedores, alianzas y canales de distribución financiera. En un ecosistema de pagos digitales inclusivo, es importante que todas las partes interesadas contribuyan para asegurar que los pagos digitales se realicen de manera responsable.

Las prácticas para pagos digitales responsables de la Alianza Better Than Cash presentan ocho buenas prácticas para la prestación de servicios a clientes que envían o reciben pagos digitales y que han sido anteriormente excluidos o marginados del sistema financiero.

Las prácticas se orientan sobre todo hacia los proveedores de servicios financieros en el diseño y prestación de sus pagos y servicios. Las prácticas también pueden usarse como una lista práctica de verificación (sujeta a la legislación pertinente) útil para:

» los reguladores al ponderar sus reglas;

» el sector privado (como en el caso de empresas de rápido movimiento de bienes y empresas de transporte) en la selección de los proveedores de pagos;

» los donantes y las organizaciones de desarrollo para la adquisición de servicios de los proveedores de pago; y

» todos los interesados en la promoción de medidas adecuadas de protección de los consumidores.

Las prácticas se enfocan en las categorías comunes de servicios de pagos digitales, ofrecidos a los mercados desatendidos financieramente, tales como las cuentas de transacciones de dinero electrónico. Las prácticas son neutrales en términos de tecnología y de proveedores, y están diseñadas para aplicarse a las innovaciones actuales en el área de pagos digitales, aunque se reconoce que podrían ser revisadas y actualizadas periódicamente. Cada práctica incluye ejemplos de lo que un cliente podría esperar en un mercado de pagos digitales responsable.

Desde su fundación en 2012, la Alianza Better Than Cash ha participado junto a los actores interesados en una variedad de foros con el objetivo primordial de que los pagos digitales se ofrezcan de manera responsable y en beneficio del destinatario y el remitente. Estas prácticas representan la culminación de varios años de consultas con los actores interesados del sector, muchas de las cuales tuvieron lugar en el marco de una serie de reuniones mundiales, como el Global Finanical Inclusion Forum (Foro Mundial de Inclusión Financiera) 2013-2020 y las deliberaciones mundiales del Responsible Finance Forum (Foro sobre Finanzas Responsables) sobre las finanzas digitales en 2014 y 2015, y su reunión regional de 2016, que se llevaron a cabo en conjunto con las reuniones de la Alianza Mundial para la Inclusión Financiera, a petición del G20. Esto a partir del reconocimiento logrado después de la crisis financiera sobre la importancia de las prácticas responsables de inclusión financiera, tal como lo consignan los Principios de Inclusión Financiera Innovadora del G20 (2010).

Hay otras prácticas que provienen de los principios, normas y códigos tratados en el documento *Better Than Cash Alliance Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services (Alianza Better Than Cash: Documentación de principios, estándares y códigos de conducta en los servicios financieros digitales)*[1] así como de otras investigaciones e informes internacionales recientes.[2] Estas prácticas han sido compartidas ampliamente en forma de borrador, y los comentarios y sugerencias producto de ese proceso se han incorporado en este documento público.

Las prácticas procuran ofrecer una herramienta útil a todos los interesados que apoyan usos responsables en la transición de los pagos en efectivo a pagos digitales con el fin de reducir la pobreza, impulsar el crecimiento inclusivo y contribuir a una mayor participación económica de las mujeres.

Prácticas

1 Dar a los clientes un trato justo

Si se pretende que los clientes confíen en los pagos digitales, se les debe brindar un trato justo, especialmente a aquellos clientes con bajos niveles de capacidad financiera y tecnológica.

2 Proteger los fondos de los clientes

Los clientes, en especial los que sufren exclusión y marginación financiera, necesitan acceso confiable y seguro a los fondos en las cuentas de transacciones digitales.

3 Garantizar la transparencia del producto para los clientes

Ofrecer a los clientes información transparente exige especial atención en un entorno digital, especialmente en contextos donde la información sólo está disponible por vía electrónica, como a través de un teléfono móvil.

4 Diseñar de acuerdo con las necesidades y capacidades de los clientes

Diseñar pagos digitales para abordar las necesidades, los roles económicos y las capacidades de los clientes, en especial de las mujeres, aumentará la conveniencia y el uso.

5 Apoyar el acceso y el uso de los clientes a través de la interoperabilidad

Si bien se debe reconocer que hay que mantener el equilibrio entre la competencia y la innovación, es de crucial importancia garantizar la interoperabilidad entre plataformas, agentes y clientes a fin de que los clientes de distintos planes pueden realizar pagos entre sí y los agentes pueden trabajar con distintos proveedores. Esto es particularmente importante para los clientes que viven en zonas rurales remotas.

6 Asumir la responsabilidad de los proveedores de servicios al cliente en toda la cadena de valor

Los clientes confiarán en los pagos digitales y los realizarán con mayor frecuencia si los proveedores asumen la responsabilidad de las acciones de los agentes, empleados y proveedores de servicios de terceros en toda la cadena de valor.

7 Proteger los datos de los clientes

La protección de los datos digitales de los clientes se ha convertido en un asunto crecientemente importante debido al volumen, velocidad y variedad de datos que se utilizan para mercadeo y calificación de crédito, y a su vez se debe reconocer que el uso de los datos de los clientes puede aumentar la gama de productos a los que estos pueden tener acceso.

8 Proporcionar recursos a los clientes

Los clientes necesitan tener acceso a un sistema de recursos adecuado para manejar los reclamos relacionados con pagos digitales. Esto es especialmente necesario en caso de quejas sobre productos innovadores y desconocidos ofrecidos a través de canales nuevos, y para clientes que vivan en lugares apartados y tengan poco o ningún contacto directo con los proveedores

7 Dar a los clientes un trato justo

"Queremos que nuestros clientes, que en su mayoría no tienen experiencia con bancos y para quienes los pagos digitales son algo nuevo, se sientan respetados y reciban un trato justo al tiempo que nuestros agentes y puntos de servicio les ofrezcan una atención especial".

SR. DASGUPTA ASIM KUMAR,
ASESOR DE RELACIONES REGULATORIAS DE BKASH LIMITED

Si el objetivo es que los clientes confíen en los pagos digitales, se les debe brindar un trato justo, especialmente a aquellos con bajos niveles de capacidad financiera y tecnológica.

ALGUNAS MANERAS EN LAS QUE SE PUEDE OFRECER UN TRATO JUSTO A LOS CLIENTES SON:

1. Toda la **publicidad y otra información de ventas** se comunica por medio de lenguaje y términos sencillos, claros, precisos y no confusos.
2. Los plazos de los productos ofrecen un equilibrio razonable entre los intereses de los clientes y del proveedor.
3. Se les da un trato respetuoso a los clientes; por ejemplo, sólo se les venden productos digitales que realmente necesitan.
4. Los requisitos de identificación son apropiados para los clientes, para facilitar el acceso.
5. Los clientes reciben el mismo trato y se evita la discriminación injusta. Como ejemplo, los proveedores no discriminan por razones de género, religión, origen étnico, afiliación política, orientación sexual, edad, residencia o algún tipo de discapacidad.
6. En caso de que se pierdan o roben dispositivos de acceso, credenciales de seguridad o la identidad de los clientes, los proveedores compensarán al cliente por cualquier transacción que se produzca después de que éste haya informado la pérdida o robo al proveedor. Igualmente, se paga compensación en la medida que una transacción supere un límite diario o periódico.
7. Se compensa a un cliente por cualquier cuota de pago que se retrase por incapacidad para realizar el pago debido a una interrupción programada en el sistema que no se haya informado al cliente.
8. Si un cliente inicia un pago digital en medio de un corte de energía, el proveedor lo procesa tan pronto como sea posible.

Proteger los fondos de los clientes

"Debido a que la confianza en los pagos digitales es esencial para lograr su eficaz realización y adopción, deben establecerse marcos normativos adecuados y proporcionales para garantizar que los fondos de los clientes estén protegidos en todo momento".

SRA. PIA ROMAN TAYAG,
JEFA DE PROMOCIÓN DE FINANZAS INCLUSIVAS DE BANGKO NG PILIPINAS

Los clientes, en especial los que sufren exclusión y marginación financiera, necesitan acceso confiable y seguro a los fondos en las cuentas de transacciones digitales.

ALGUNAS MANERAS EN QUE SE PUEDEN PROTEGER LOS FONDOS QUE LOS CLIENTES TIENEN EN CUENTAS PARA TRANSACCIONES DIGITALES SON:

1. **Fondos de contrapartida:** los proveedores que no estén sujetos a regulación prudencial mantienen en cuentas separadas, en instituciones prudencialmente reguladas, una cantidad de fondos igual al total de los saldos pendientes. Como alternativa, los fondos de contrapartida se podrían invertir en otros valores permisibles (por ejemplo en títulos del gobierno con un mercado secundario activo). Lo ideal es que las cuentas e inversiones se mantengan para el beneficio de los clientes (como en una cuenta de fideicomiso). Los fondos de contrapartida sólo se utilizan para hacer pagos a clientes y no para fines operativos. Están protegidos contra reclamaciones de acreedores de terceros del proveedor. Los supervisores pueden acceder a registros de cuentas e inversiones en tiempo real, cuando esto sea factible.
2. **Capacidad y seguridad de sistemas:** se toman fuertes medidas contra el fraude, la piratería electrónica y cualquier otra forma de uso no autorizado para garantizar la confiabilidad de la red y la capacidad del sistema, así como la seguridad de la red de pagos y de los canales de entrega.
3. **Fraude:** el cliente recibe compensación del proveedor por cualquier pérdida directa debida a fraude cometido por agentes, empleados y proveedores de servicios terceros (como los administradores de su red de agentes) y por fraude de terceros ocasionado por una violación de seguridad razonablemente prevenible. Igualmente debe informarse a los clientes sin demora sobre cualquier sospecha de fraude.
4. **Transacciones erróneas y no autorizadas:** la interfaz del usuario se diseña para que sea clara, simple y segura. Además se pide confirmación de la información de pago antes de completar una transacción. El objetivo es minimizar el riesgo de transacciones erróneas y no autorizadas, así como simplificar el acceso.

Garantizar la transparencia del producto para los clientes

"Todo aquello que valga la pena ofrecer debe ofrecerse de manera transparente. Esto es aún más importante para las personas que realicen y reciban pagos digitales por primera vez. Es deber de los proveedores darles a las personas la información clara y completa necesaria para tomar las mejores decisiones".

DR. BITANGE NDEMO,
PROFESOR ADJUNTO DE LA ESCUELA DE NEGOCIOS DE LA UNIVERSIDAD DE NAIROBI Y EXSECRETARIO PERMANENTE DEL MINISTERIO DE INFORMACIÓN Y COMUNICACIÓN DE KENYA

Ofrecer a los clientes información transparente exige especial atención en un entorno digital, especialmente cuando la información sólo está disponible electrónicamente, como en un teléfono celular.

EJEMPLOS DE CÓMO MEJORAR LA TRANSPARENCIA DE UN PRODUCTO EN UN ENTORNO DIGITAL INCLUYEN:

1. **Información del producto:** cada cliente tiene acceso (el cual puede ser en formato digital) a una declaración clara, simple y fácilmente comparable de características del producto, términos, honorarios y cualquier interés pagable. Esto se hace antes de que el servicio de pagos sea proporcionado. La información se mantiene actualizada y está en un formato en el que el cliente puede mantenerla y/o acceder, incluso digitalmente. El proveedor también puede explicar la información al cliente si éste lo solicita o si parece que no la comprende (por ejemplo, si está en un idioma que no domina).

2. Registros de transacción y de la cuenta: el cliente recibe un comprobante de cada transacción y tiene fácil acceso a registros claros y simples de las transacciones y de la cuenta, los cuales pueden ser proporcionados digitalmente. Estos registros también tienen que estar en un formato en el que el cliente pueda mantener o acceder a la información, como un historial de transacciones digitales.

4 Diseñar de acuerdo con las necesidades y capacidades de los clientes

"La experiencia de los clientes de BIM es que nuestro producto les resulta transparente, intuitivo y fácil de usar. Esto es así porque hemos diseñado BIM pensando en las necesidades y capacidades de los clientes".

DRA. CAROLINA TRIVELLI, DIRECTORA GENERAL DE PAGOS DIGITALES PERUANOS

Diseñar pagos digitales para abordar las necesidades, los roles económicos y las capacidades de los clientes, en especial de las mujeres, aumentará la conveniencia y el uso.

ALGUNAS ACCIONES PERTINENTES PARA EL DISEÑO DE SERVICIOS DE PAGOS DIGITALES SON:

1. **Diseño de servicios de pago:** los servicios de pagos digitales se diseñan a partir de investigación en cuanto a las necesidades, preferencias y comportamiento de los clientes. Su diseño también toma en cuenta los niveles de capacidad financiera y tecnológica de los clientes y, sobre todo en el caso de mercados desatendidos, es sencillo y claro. Debido al mayor nivel de exclusión de las mujeres, es particularmente importante que los servicios de pagos se diseñen con el objetivo de cubrir las necesidades de las mujeres y teniendo en cuenta sus necesidades y roles económicos.
2. **Apoyo a los usuarios:** cada cliente de un servicio de pagos digitales recibe:
   - **(a)** Instrucciones fáciles de entender sobre el modo de utilizar el servicio y proteger sus credenciales de seguridad (contraseñas y PIN), además de una descripción de las responsabilidades del cliente.
   - **(b)** Acceso a una línea directa de 24 horas para notificar al proveedor sobre un dispositivo de acceso o credenciales de seguridad extraviadas o robadas, una transacción errónea o no autorizada o una violación de la seguridad.
   - **(c)** Información de contacto del proveedor durante horario de oficina para así contar con una fuente confiable de información sobre el modo de utilizar un servicio financiero digital y sus características.
   - **(d)** Apoyo adicional a los usuarios primerizos (particularmente a las mujeres),según sea necesario y viable, para garantizar el uso y adopción seguros.

5 Apoyar el acceso y el uso de los clientes a través de la interoperabilidad

"El regulador tiene una labor de generar sistemas de pago interoperables que puedan ayudar a reducir los costos de transacción de los clientes y mejorar la conveniencia".

SR. SETTOR AMEDIKU
DIRECTOR DEL DEPARTAMENTO DE ESTABILIDAD FINANCIERA DEL BANCO DE GHANA.

Si bien se debe reconocer que hay que mantener el equilibrio entre la competencia y la innovación, tiene mucho sentido garantizar la interoperabilidad entre plataformas, agentes y clientes a fin de que los clientes de distintos planes pueden realizar pagos entre sí y los agentes pueden trabajar con distintos proveedores. Esto es particularmente importante para los clientes que viven en zonas rurales remotas.

ALGUNAS MANERAS DE FACILITAR LA INTEROPERABILIDAD SON:

1. Fomentar las iniciativas de interoperabilidad de colaboración dirigidas por el sector a fin de garantizar que los clientes realicen transacciones financieras digitales independientemente de donde vivan o quién sea su proveedor.
2. Desalentar cualquier obstáculo deliberado a la interoperabilidad (tales como los acuerdos de exclusividad de agentes).

6 Asumir la responsabilidad de los proveedores de servicios al cliente a través de la cadena de valor

"Sólo podemos ganarnos la confianza de los clientes si nosotros, como proveedores de servicios, nos aseguramos de que todos los participantes de nuestra cadena de valor estén actuando responsablemente, y que tengamos los sistemas y procesos para asegurar que eso suceda. Este es el mensaje que se debe dar a los clientes, particularmente a aquellos que utilizan los pagos digitales por primera vez".

SR. RAJPAL DUGGAL
SERVICIOS OXIGEN INDIA

Los clientes confiarán en los pagos digitales y los realizarán con mayor frecuencia si los proveedores asumen la responsabilidad de las acciones de los agentes, empleados y proveedores de servicios de terceros en toda la cadena de valor.

ALGUNAS MANERAS DE ASUMIR LA RESPONSABILIDAD POR LOS AGENTES, EMPLEADOS Y PROVEEDORES DE SERVICIOS DE TERCEROS SON:

1. **Responsabilidad:** los agentes, empleados y los proveedores de servicios de terceros están debidamente capacitados (incluso en las características de los productos y en las responsabilidades normativas).
2. **Capacitación y supervisión:** los agentes y empleados y los proveedores de servicios terceros están debidamente capacitados (incluso en las características de los productos y en las responsabilidades normativas) y se les supervisa adecuadamente, incluso en lo relativo a las características del producto, las responsabilidades normativas y la conducta relativa a las cuestiones de género. Además cuentan con los recursos necesarios para prestar servicios de pagos de manera competente y legal.
3. **Datos del proveedor:** los agentes entregan a los clientes el nombre y la información de contacto del proveedor cuando estos abren su cuenta y en cualquier momento en que la soliciten.

7 Proteger los datos de los clientes

"Junto al aumento de la inclusión financiera, se hace crecientemente crucial proteger la gran cantidad de datos que manejan los distintos proveedores financieros inclusivos".

DR. TAO SUN
DIRECTOR EN JEFE
DE ANT FINANCIAL

La protección de los datos digitales de los clientes se ha convertido en un asunto crecientemente importante debido al volumen, velocidad y variedad de datos que se utilizan para mercadeo y calificación de crédito, y a su vez se debe reconocer que el uso de los datos de los clientes puede aumentar la gama de productos a los que estos pueden tener acceso.

ALGUNAS MANERAS EN LAS QUE SE PUEDEN PROTEGER LOS DATOS PERSONALES DE LOS CLIENTES EN UN ENTORNO DIGITAL A NIVEL BÁSICO SON:

1. **Confidencialidad y seguridad:** se toman medidas razonables para garantizar la confidencialidad y seguridad de los datos pertinentes del cliente en las transacciones de pago digitales. Tales datos incluyen, entre otros, la información de identificación y del contrato; historiales de transacciones; credenciales de seguridad; uso de datos en dispositivos, teléfono celular e internet, y datos de geolocalización. Con el consentimiento expreso e informado de los clientes, se pueden usar y divulgar los datos para fines específicos, tales como la promoción de nuevos servicios.
2. **Historial de auditoría:** se pone a la disposición de los clientes y supervisores un claro historial de auditoría de registros de transacciones.

8 Proporcionar recursos a los clientes

"La experiencia de México es que mecanismos de recursos eficaces que funcionen en un entorno digital son fundamentales para generar confianza en los clientes en el uso de servicios financieros".

SRA. MARÍA FERNANDA TRIGO, DIRECTORA GENERAL DE ACCESO A SERVICIOS FINANCIEROS DE LA COMISIÓN NACIONAL BANCARIA Y DE VALORES DE MÉXICO

Los clientes deben tener acceso a un sistema de recursos adecuado para manejar las reclamaciones relacionadas con pagos digitales. Esto se torna particularmente necesario en caso de quejas sobre productos innovadores y desconocidos ofrecidos a través de canales nuevos, y para clientes que vivan en lugares apartados y tengan poco o ningún contacto directo con los proveedores.

ALGUNOS SISTEMAS DE RECURSOS EFICACES PARA CLIENTES DE PAGOS DIGITALES INCLUYEN:

1. **Quejas:** los clientes pueden acceder fácilmente a un sistema de quejas transparente, eficiente y gratuito o a bajo costo. Este sistema debe ser accesible para todos, independientemente de las normas culturales, el idioma, la movilidad, etc. El sistema es accesible por vía telefónica o digital (una página web o un mensaje de texto), o visitando la sede del proveedor.
2. **Disputas:** los clientes también tienen acceso a un servicio de terceros independiente que se ocupa de las disputas con los proveedores en los casos en que el proveedor no haya abordado y resuelto la queja del cliente de manera adecuada. Este sistema de terceros es de fácil acceso (incluso por vía telefónica o digital), transparente, eficiente y gratuito o de bajo costo.
3. **Información sobre sistemas de recursos:** la información sobre los términos y condiciones del sistema de recursos de un proveedor se encuentran en el sitio web del proveedor y en las instalaciones del proveedor y el agente. Además, cuando un cliente hace una denuncia recibe una copia de esta información, que puede entregarse en formato digital.
4. **Datos de las quejas:** los proveedores llevan registros de quejas de los clientes y su respuesta a cada queja. Los reguladores también reciben informes periódicos de los datos de las quejas. Se publican los problemas sistémicos del sector, pero teniendo cuidado de no revelar la identidad de los denunciantes.

Información general

PRÁCTICA 1: Dar a los clientes un trato justo

Para confiar en los pagos digitales, los clientes deben brindar un trato justo, especialmente a aquellos clientes con bajos niveles de capacidad fInanciera y tecnológica.

ALGUNAS MANERAS EN LAS QUE SE PUEDE OFRECER UN TRATO JUSTO A LOS CLIENTES SON:

1. Toda la publicidad y otra información de ventas se comunica mediante lenguaje y términos sencillos, claros, precisos y no confusos.
2. Los plazos de los productos ofrecen un equilibrio razonable entre los intereses de los clientes y del proveedor.
3. Se les da un trato respetuoso a los clientes; por ejemplo, sólo se les venden productos digitales que realmente necesitan.
4. Los requisitos de identificación son apropiados para los clientes, para facilitar el acceso.
5. Los clientes reciben el mismo trato y se evita la discriminación injusta. Como ejemplo, los proveedores no discriminan por razones de género, religión, origen étnico, afiliación política, orientación sexual, edad, residencia o algún tipo de discapacidad.
6. En caso de que se extravíen o roben dispositivos de acceso, credenciales de seguridad, o la identidad de los clientes, los proveedores compensarán al cliente por cualquier transacción que se produzca después de que el cliente haya informado la pérdida o el robo al proveedor. Igualmente, se paga compensación en la medida que una transacción supere un límite diario o periódico.
7. Se compensa a un cliente por cualquier cuota de pago exigible que se retrase por incapacidad para realizar el pago debido a una interrupción programada en el sistema que no se haya informado al cliente.
8. Si un cliente inicia un pago digital en medio de un corte de energía, el proveedor lo procesa tan pronto como sea posible.

ANTECEDENTES

Para confiar en los pagos digitales, los clientes deben recibir un trato justo. Esto es especialmente importante para los clientes que tienen poca o ninguna experiencia en el uso de servicios financieros, una categoría que incluye a las mujeres de manera desproporcionada, en virtud de la desigualdad en el acceso debida a cuestiones de género. Un ejemplo de este enfoque se encuentra en los *Principios de alto nivel de protección al consumidor financiero,* en particular en el principio 3, que precisa que: "Todos los consumidores financieros deben recibir un trato equitativo, honesto y justo en todas las etapas de su relación con proveedores de servicios financieros. Debe prestarse especial atención a las necesidades de los grupos vulnerables".[3]

1.1 Publicidad y otra información de ventas

La práctica 1.1 es similar en foco a la norma 3 del principio 1 de la nueva versión de las Normas de Certificación de Protección de Clientes de The Smart Campaing, la cual aboga por "una política y un proceso documentado para prevenir técnicas de ventas agresivas y de firmas forzosas de contratos".

La práctica 1.1 podría cubrir todos los materiales promocionales a los que tenga acceso un cliente real o potencial a través de cualquier medio de comunicación, así como la información que figure en folletos promocionales y aquella que faciliten agentes y empleados.

1.2 Los plazos de los productos ofrecen un equilibrio entre los intereses de los clientes y los del proveedor

Parte del trato justo a los clientes consiste en asegurar que los términos y las condiciones de los pagos digitales estándar no saquen ventaja desleal de los clientes. Ejemplos de términos injustos incluyen cláusulas que hacen que el cliente sea responsable de todos los pagos erróneos (incluso después de que se le haya avisado) o que establecen que el proveedor no tiene responsabilidad

alguna sobre sus agentes ni se hace responsable ante su propia imposibilidad de prestar el servicio por el cual el cliente está pagando.

La Reglamentación Número 16/1/PBI/2014 del Banco de Indonesia sobre protección de los consumidores de sistemas de pago (en adelante, **Reglamentación de Indonesia sobre protección de los consumidores de sistemas de pago**) es un ejemplo de reglamentos específicos sobre pagos que tratan el tema de cláusulas abusivas.[4]

1.3 Trato respetuoso a los clientes

Tal como se señaló en el principio 5 de los Principios de protección al cliente de *The Smart Campaign*, el respeto al cliente siempre va acompañado del trato justo. Hay muchas maneras de demostrar respeto a los clientes, tales como venderles únicamente productos adecuados a sus necesidades y capacidades. A modo de ejemplo, para mostrar respeto, no se debe presionar a un cliente potencial para que adquiera un producto de pagos digitales sin considerar si el producto es adecuado a sus necesidades de pago, y no se debe alentar la adopción de dichos productos en zonas en las que el cliente carezca de fácil acceso a una red de agentes para servicios de efectivo. Otro ejemplo es evaluar si un cliente de una cuenta de transacción digital puede realmente pagar un microcrédito vinculado antes de ofrecerle el préstamo. En todo caso, las clientas deben recibir un trato tan respetuoso como el que reciben los clientes.

1.4 Requisitos de identificación del cliente

Los clientes con bajos ingresos no necesariamente cuentan con formas de identificación tradicional, como un documento nacional de identificación, un permiso de conducir, pasaporte, acta de nacimiento o una dirección postal. Por esta única razón podría negárseles el acceso a servicios de pagos digitales.

Sin embargo, las *Recomendaciones del Grupo de Acción Financiera (GAFI): Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y de la proliferación* (en adelante, las ***Recomendaciones del GAFI***) revisadas en 2012, que sirven de base a leyes nacionales contra el lavado de activos y contra el terrorismo, exigen el uso de requisitos de identificación del cliente basados en riesgos.[5]

Un servicio de pagos, como una cuenta de dinero electrónico, podría ser un ejemplo de un producto de ese tipo, dependiendo de factores tales como los límites en las transacciones y los saldos. Las pautas de la GAFI sobre la obligación de verificar la identidad de un cliente también dejan claro que no es necesario contar con documentos de identificación emitidos por el gobierno (de los cuales muchos clientes de bajos ingresos carecen) y señalan que "la flexibilidad es particularmente importante para la inclusión financiera".[6]

1.5 Discriminación

La prácrica 1.5 es similar al Estándar 2 del principio 5 de los **Estándares de certificación en protección al cliente de *The Smart Campaign*** (en adelante, los Estándares de certificación de *The Smart Campaign*) que, en resumen, procuran limitar la discriminación por motivos de origen étnico, género, edad, discapacidad, afiliación política, orientación sexual, casta y religión.

1.6 Dispositivo de acceso, credenciales de seguridad o identidad perdidas o robadas

La práctica 1.6 propone compensar cualquier transacción que se produzca después de que se haya informado al proveedor la pérdida o robo además de en los casos en que el monto de la transacción supere un límite de transacciones diario o periódico. Este enfoque es similar al que se aprecia, por ejemplo, en el ePayments Code (Código de Pagos Electrónicos), administrado por la Comisión Australiana de Valores e Inversiones (en adelante, **Código de pagos electrónicos de Australia**), si bien ese código tiene un enfoque más complejo para la asignación de responsabilidades.[7]

1.7 Interrupciones del sistema

El Enfoque del Grupo Consultivo de Ayuda a la Población más Pobre (GCAP) sobre finanzas digitales bien implementadas: razones para mejorar la mitigación de los riesgos de los clientes (en adelante, **Enfoque del GCAP sobre finanzas digitales**) identificó la "Imposibilidad de realizar operaciones debido a las interrupciones de las redes o los servicios" como el primero de siete riesgos principales que enfrentan los consumidores.[8]

Las interrupciones del sistema son una preocupación común de los clientes. Es lógico que los clientes esperen tener acceso a fondos en cuentas de pagos digitales cuando los necesiten. Esto es especialmente importante en el caso de clientes con bajos ingresos que podrían no tener acceso a otras fuentes de fondos. No obstante, estas prácticas proponen que los clientes sólo pueden esperar de modo realista que se compense la pérdida directa de una cuota de pago exigible debido a una interrupción del sistema de la que no tenían aviso previo (en lugar de las pérdidas indirectas, como las derivadas de una pérdida de beneficios comerciales).

Un enfoque más amplio en torno al problema de las interrupciones del sistema lo proporciona la cláusula 14.2 del Código de pagos electrónicos de Australia, que establece que un suscriptor no debe negar el derecho del usuario a reclamar daños indirectos ocasionados por el mal funcionamiento de un sistema o equipo proporcionado por cualquiera de las partes de una red electrónica compartida (a menos que el cliente razonablemente debiera haber sido consciente con anticipación del mal funcionamiento o interrupción).[9]

1.8 Cortes de energía

La práctica 1.8 aborda el problema común de los cortes de energía que afectan a los pagos digitales. En dichos casos, los clientes deben contar con una garantía de que los pagos que fueron iniciados pero no recibidos se procesarán tan pronto como sea posible.

PRÁCTICA 2: Proteger los fondos de los clientes

Los clientes, en especial los que sufren exclusión y marginación financiera, necesitan acceso confiable y seguro a los fondos en las cuentas de transacciones digitales.

ALGUNAS MANERAS EN LAS QUE SE PUEDEN PROTEGER LOS FONDOS QUE LOS CLIENTES TIENEN EN CUENTAS PARA TRANSACCIONES DIGITALES SON:

1. **Fondos de contrapartida:** los proveedores que no estén sujetos a regulación prudencial mantienen en cuentas separadas, en instituciones prudencialmente reguladas, una cantidad de fondos igual al total de los saldos pendientes. Como alternativa, los fondos de contrapartida se podrían invertir en otros valores permisibles (por ejemplo en títulos del gobierno con un mercado secundario activo). Lo ideal es que las cuentas e inversiones se mantengan para el beneficio de los clientes (como en una cuenta de fideicomiso). A su vez, están protegidos contra reclamaciones de acreedores terceros del proveedor. Los supervisores pueden acceder a registros de cuentas e inversiones en tiempo real allí donde sea factible.
2. **Capacidad y seguridad del sistema:** se toman medidas sólidas para garantizar la confiabilidad de la red y la capacidad del sistema, así como la seguridad de la red de pagos y de los canales de entrega contra fraude, piratería electrónica y cualquier otra forma de uso no autorizado.
3. **Fraude:** el cliente recibe compensación del proveedor por cualquier pérdida directa debido a fraude cometido por agentes, empleados y proveedores de servicios de terceros (como los administradores de su red de agentes) y por fraude de terceros ocasionado por una violación de seguridad razonablemente prevenible. Igualmente debe informarse a los clientes sin demora sobre cualquier sospecha de fraude.
4. **Transacciones erróneas y no autorizadas:** la interfaz del usuario se diseña para que sea clara, simple y segura. Además se pide confirmación de la información de pago antes de completar la transacción. El objetivo es minimizar el riesgo de transacciones erróneas y no autorizadas, así como simplicar el acceso.

ANTECEDENTES

2.1 Fondos de contrapartida

El riesgo fundamental que enfrentan los clientes que usan un producto de pagos digitales es no poder acceder a sus fondos cuando los necesiten. En efecto, el enfoque del GCAP sobre finanzas digitales presenta como un riesgo fundamental la "falta de liquidez o de efectivo en caja de los agentes, lo que también afecta la capacidad de realizar operaciones".

También existe el riesgo de que el proveedor, o su banco, se hagan insolventes. Por último, los riesgos operativos generales podrían afectar la capacidad de los clientes para realizar operaciones.[10]

De manera particular, la práctica 2 de la Alianza Better Than Cash proporciona los siguientes ejemplos de buenas prácticas:

- La asignación de fondos de contrapartida de los saldos de fondos y valores no debe obstaculizarse, lo cual quiere decir que no se deben utilizar dichos fondos de contrapartida como garantía para otras deudas.
- Los fondos de contrapartida se pueden mantener en una cuenta en una institución prudencialmente regulada (como una cuenta de fideicomiso) o en otras inversiones permitidas (como títulos del gobierno).
- Los fondos de contrapartida sólo se utilizan para realizar pagos a clientes y deben estar protegidos contra demandas de acreedores terceros a fin de resguardarlos de los riesgos de insolvencia e iliquidez.

Son numerosos los ejemplos de principios, normas y códigos, y de legislación nacional, que tratan de proteger el encaje adecuado de los fondos de los clientes en cuentas de pagos digitales. Entre dichos ejemplos se cuentan:

- El principio rector 2 de los *Aspectos de Pagos de la Inclusión Financiera (PAFI),* un informe del Comité de Pagos e Infraestructura de Mercado y el Banco Mundial (en adelante, el Informe PAFI).
- El principio 1 del *Código de Conducta del GSMA.*
- La legislación y prácticas en países como Afganistán, Kenya, Malawi, Filipinas y Tanzania.[11]

Cada uno de estos ejemplos enfoca este asunto fundamental de distintas maneras, pero todos abordan el tema esencial de la protección de los fondos de los clientes.

2.2 Capacidad y seguridad de sistemas

Es lógico que los clientes esperen que la capacidad y la seguridad de los sistemas de pagos digitales se enfoque de manera sólida y continua. El informe PAFI hace hincapié en la necesidad de contar con puntos de acceso y canales confiables y de alta calidad (véase el Principio Rector 5). El *Código de Conducta del GSMA* contiene disposiciones detalladas sobre seguridad y capacidad de sistemas (véase especialmente las prácticas 4 y 5), que también pueden encontrarse en el Principio Rector 3 en el informe PAFI y en la *Guía de Level One Project* de la Fundación Bill y Melinda Gates (en adelante, ***Guía de Level One Project* de la Fundación Gates**).

Finalmente, estas preocupaciones han sido abordadas a nivel nacional. A modo de ejemplo, la Circular No 649 de 2009 de Filipinas sobre dinero electrónico exige que se adopten políticas y medidas de seguridad adecuadas para proteger la integridad, autenticidad y confidencialidad de los datos y los sistemas operativos.[12] La reglamentación de Indonesia sobre protección de los consumidores de sistemas de pago también aborda cuestiones de seguridad.[13] El nuevo Marco de Protección de los Consumidores de Nigeria es más específico, pues dispone que el Banco Central "especifique los estándares tecnológicos mínimos de las plataformas de pago.[14]

Los clientes también pueden contar con que los pagos digitales se realicen de manera inmediata, en tiempo real. No obstante, estas prácticas no abordan este asunto, ya que no todos los sistemas de pago pueden liquidar las transacciones en tiempo real. Para ver prácticas sobre la liquidación de pagos en tiempo real, consulte la práctica 1.2.1 de la Guía de *Level One Project* de la Fundación Gates sobre transferencias inmediatas de fondos y liquidaciones de pagos el mismo día, así como la práctica 1.2.1 del Código de Conducta del GSMA, ya que ambos recursos hacen referencia a cargos y abonos de dinero en tiempo real.

2.3 Fraude

La mayoría de los clientes espera ser compensado por el proveedor en caso de fraudes cometidos por empleados, agentes y proveedores de servicios terceros. Los clientes también pueden esperar recibir compensación en caso de fraude que surja de violaciones de la seguridad que se hayan podido

evitar razonablemente (como las ocasionadas por un hacker tercero). En algunos aspectos, la práctica 2.3 podría parecer onerosa. Sin embargo, el fraude es un riesgo importante para los clientes, tal como se destacó en el *Informe de resultados sobre las finanzas digitales responsables del V Foro sobre finanzas responsables (en adelante,* ***Informe de resultados del V Foro sobre finanzas responsables).*** Los clientes por lo general esperan que los proveedores de los servicios de pago asuman la responsabilidad de los fraudes que puedan cometer las personas y entidades que se encuentren (o que deban estar) bajo su control.

Como se señaló en el preámbulo a la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo del 25 de noviembre de 2015 sobre servicios de pago en el mercado interno (en adelante, **PSD2**): "Todos los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, gracias a la adopción de tecnologías que permitan garantizar una autenticación segura del usuario y minimizar el riesgo de fraude".[15] La PSD2 contiene disposiciones muy fuertes en apoyo a los usuarios que afirmen que no han autorizado una transacción.[16]

La necesidad de tomar medidas para prevenir el fraude también es un tema que se trata de manera sostenida en la Guía de *Level One Project* de la Fundación Gates y en otros foros y publicaciones. Así, por ejemplo, el Enfoque del GCAP sobre finanzas digitales identifica como un riesgo clave el "fraude dirigido a los clientes", y el informe de resultados del V Foro sobre finanzas responsables identificó el fraude como una zona de riesgo fundamental que debe abordarse.

2.4 Transacciones erróneas y no autorizadas

La mayoría de los expertos y comentaristas está de acuerdo en que los sistemas de pagos digitales deben tener una interfaz clara y fácil de usar para reducir el riesgo de transacciones erróneas y para fomentar el uso continuo de los servicios de pago. El enfoque del GCAP sobre finanzas digitales destaca como riesgo clave las "Interfaces de usuario que a muchos podrían parecer complejas y confusas".

El Informe sobre evidencia e innovación para ampliar las finanzas digitales inclusivas del **VI Foro sobre finanzas responsables** (en adelante, Informe del VI Foro sobre finanzas responsables) también aborda la importancia de interfaces fáciles de usar.

Las transacciones no autorizadas son también una preocupación importante para los clientes que esperan que las interfaces de usuario sean seguras. La PSD2 pone una fuerte responsabilidad en el proveedor con respecto a las transacciones que el usuario afirme que no fueron autorizadas o que se ejecutaron de manera incorrecta.[17]

PRÁCTICA 3: Garantizar la transparencia del producto para los clientes

Ofrecer a los clientes información transparente exige especial atención en un entorno digital, especialmente en contextos en los que la información solo está disponible por vía electrónica, como en un teléfono móvil.

ALGUNAS MANERAS EN LAS QUE SE PUEDE MEJORAR LA TRANSPARENCIA DE LOS PRODUCTOS EN UN ENTORNO DIGITAL SON:

1. **Información del producto:** cada cliente recibe acceso (que puede ser digital) a una exposición clara, sencilla y fácilmente comparable de características, condiciones, tasas e intereses exigibles de los productos. Esto se hace antes de que se preste el servicio de pago. La información se mantiene actualizada y en un formato que el cliente pueda conservar o acceder, incluidos los formatos digitales. El proveedor también explica la información al cliente si éste lo solicita, o si es evidente que no la comprende (por ejemplo, si está en un idioma que no domina).
2. **Registros de transacciones y cuentas:** un cliente recibe comprobante de cada transacción y cuenta con un acceso fácil a registros claros y simples de transacciones y cuentas. Estos registros podrían proporcionarse en forma digital. Del mismo modo deben entregarse en formato que el cliente pueda conservar o acceder, como en el caso de un historial de transacciones digitales.

ANTECEDENTES

3.1 Información de los productos

La información de productos clara y fácil de entender ayuda al desarrollo de una clientela informada, que suele confiar en los pagos digitales y los usa. También permite realizar comparaciones de productos y puede fomentar la competencia y reducir los costos. Sin embargo, la información no resulta útil si es larga y compleja y los clientes no la entienden.

Por otro lado, la información proporcionada en la pequeña pantalla de un celular puede resultar insuficiente, como se señaló en el Informe de resultados del *V Foro sobre finanzas responsables.* En cualquier caso, la información debe ser accesible para referencia futura, como en caso de que un cliente tenga una queja. Los términos y condiciones del producto podrían facilitarse por correo electrónico, publicarse en un sitio web, o bien podrían ser entregados por un agente. La práctica 3.1 ha sido diseñada para reflejar estas consideraciones.

La importancia de la transparencia es ampliamente reconocida en otras normas y prácticas internacionales. A modo de ejemplo, un riesgo importante identificado por el *Enfoque del GCAP sobre finanzas digitales* son las "tarifas y otras condiciones no transparentes", y subraya que la "transparencia de información del producto es clave para la prestación de servicios de finanzas digitales responsables". También destaca la importancia de la información bien diseñada y comparable.

Además, los recursos que se presentan a continuación subrayan la importancia de la transparencia (en distintos grados):

- La práctica 6.1.1 del *Código de Conducta del GSMA.*
- El principio 3 de los Principios de protección al cliente de *The Smart Campaign.*
- Los principios rectores 2 y 5 del informe PAFI.

Estos últimos principios también destacan la necesidad de utilizar "metodologías comparables" y sugieren que se ofrezca información sobre los riesgos asociados con el uso de un producto y el modo de reducir al mínimo los costos mientras se aumentan al máximo los beneficios. También hay muchos ejemplos en los gobiernos nacionales, así como iniciativas legislativas en favor de la transparencia de la información sobre los productos financieros y su rendimiento. Estas iniciativas pueden aplicarse a productos de pagos digitales así como a otros tipos de servicios financieros.

Un ejemplo determinante proviene del Buró de Entidades Financieras de México.[18] El Buró publica información en su página web acerca de los productos de una institución financiera, sus honorarios y comisiones, cláusulas abusivas, reclamaciones, sanciones y otra información pertinente al rendimiento de la institución. Las instituciones financieras también están obligadas a publicar esta información en sus propios sitios web. Otros ejemplos son los requisitos de transparencia de la Reglamentación de Indonesia sobre protección de los consumidores de sistemas de pago y las disposiciones que requieren la divulgación de tasas y cargos en la Normativa sobre dinero electrónico de Tanzania de 2015.

3.2 Registros de transacciones y cuentas

Los clientes pueden esperar tener acceso continuo a transacciones y registros de cuentas claros y sencillos. Para ser útiles, estos deben presentarse en un formato que los clientes puedan comprender fácilmente y en el que puedan confiar. Estos registros revisten especial importancia si un cliente tiene una queja sobre una transacción específica. A modo de ejemplo, podría presentarse una queja sobre un pago efectuado por error o no recibido, y los registros podrían guardarse en formato digital, siempre que el cliente pueda conservar o acceder fácilmente a la información.

PRÁCTICA 4: Diseñar pensando en las necesidades y capacidades de los clientes

El diseño de pagos digitales, teniendo en cuenta las necesidades y capacidades de los clientes, permite aumentar el uso y reducir problemas y quejas.

ALGUNAS ACCIONES PERTINENTES AL DISEÑO DE SERVICIOS DE PAGOS DIGITALES SON:

1. **Diseño de servicios de pago:** los servicios de pagos digitales se diseñan a partir de investigación en cuanto a las necesidades, preferencias y comportamiento de los clientes. Su diseño también toma en cuenta los niveles probables de capacidad financiera y tecnológica de los clientes y, sobre todo en el caso de mercados desatendidos, es sencillo y claro. Debido al mayor nivel de exclusión de las mujeres, es particularmente importante que los servicios de pagos se diseñen con el objetivo de cubrir las necesidades de las mujeres y teniendo en cuenta sus necesidades y roles económicos.
2. **Apoyo a los usuarios:** cada cliente de un servicio de pagos digitales recibe:
   - **(a)** Instrucciones fáciles de entender sobre el modo de utilizar el servicio y proteger sus credenciales de seguridad (contraseñas y PIN), además de una descripción de las responsabilidades del cliente.
   - **(b)** Acceso a una línea directa de 24 horas para notificar al proveedor sobre un dispositivo de acceso o credenciales de seguridad extraviadas o robadas, una transacción errónea o no autorizada o una violación de la seguridad.
   - **(c)** Información de contacto del proveedor durante horario de oficina para así contar con una fuente confiable de información sobre el modo de utilizar un servicio financiero digital y sus características.
   - **(d)** Apoyo adicional a los primeros usuarios primerizos (particularmente a las mujeres), según sea necesario y viable, para garantizar la adopción segura y el uso.

ANTECEDENTES

4.1 Diseño del servicio de pago

Como destaca el *Informe del VI Foro sobre finanzas responsables,*[19] para ser útiles y que los clientes los usen, los servicios de pagos digitales deben diseñarse para satisfacer las necesidades de grupos de clientes a los que estén dirigidos. Igualmente, deben tenerse en cuenta las probables preferencias y comportamientos de los clientes. A modo de ejemplo, el principio 1 de los *Principios de protección al cliente* de *The Smart Campaign* trata sobre el adecuado diseño y entrega de productos, mientras que el principio rector 4 de la PAFI se refiere a la necesidad de que las transacciones y los productos de pago "cumplan una amplia gama de necesidades de operación de la población a la que estén dirigidos, a bajo costo o sin costo alguno". No obstante, las prácticas de la Alianza Better Than Cash no hacen referencia al costo de los pagos, ya que esto podría limitar la innovación y la competencia. Más bien se centran en el adecuado diseño de productos. Esto puede lograrse, por ejemplo, mediante la investigación orientada al cliente, los grupos de discusión de clientes y las encuestas, que tomen en consideración subsegmentos de mercado, incluidas las mujeres en sus distintos roles económicos.

4.2 Apoyo a los usuarios

Los clientes desatendidos que usan pagos digitales suelen tener bajos niveles de capacidad tecnológica o financiera. Esto puede desalentarlos de usar pagos digitales. Los clientes también podrían no entender los riesgos de compartir sus PIN o el modo de evitar operaciones erróneas o incluso de comprender las características de un servicio de pagos digitales y la forma de usarlo. El fomento de las capacidades de las mujeres es una inversión provechosa. La práctica 4 proporciona pasos simples y útiles sobre estos asuntos.

No obstante, la práctica 4 no pretende cubrir toda la gama de estrategias y programas sobre capacidad financiera que podrían utilizarse para pagos digitales. Esto se debe a que las prácticas de la Alianza procuran ser específicos y prácticos. Sin embargo, el principio rector 6 del Informe de la PAFI y el Banco Mundial, que trata sobre cuestiones de educación financiera, hace sugerencias específicas, tales como:

- Que los sectores público y privado realicen actividades coordinadas de educación financiera.
- Que los programas de educación financiera tengan un claro enfoque orientado a las cuentas de transacciones.
- Que la educación financiera se centre en proporcionar información sobre los tipos de cuentas que existen, los requisitos de apertura de cuentas, las tarifas pertinentes y la forma de reducir al mínimo los costos y los riesgos, además de la identificación de las medidas básicas de seguridad y de las obligaciones generales de los proveedores y usuarios.
- Que se ofrezca formación práctica como parte de la oferta de un nuevo producto.

PRÁCTICA 5: Apoyar el uso a partir de la interoperabilidad

Si bien se debe reconocer que hay que mantener el equilibrio entre la competencia y la innovación, es de crucial importancia garantizar la interoperabilidad entre plataformas, agentes y clientes a fin de que los clientes de distintos planes realicen pagos entre sí y los agentes trabajen con distintos proveedores. Esto es particularmente importante para los clientes que viven en zonas rurales remotas.

ALGUNAS MANERAS DE FACILITAR LA INTEROPERABILIDAD SON:

1. Estimular las iniciativas de colaboración e interoperabilidad dirigidas por el sector a fin de garantizar que los clientes realicen transacciones financieras digitales independientemente de donde vivan o quién sea su proveedor.
2. Desalentar cualquier obstáculo deliberado a la interoperabilidad (tales como los acuerdos de exclusividad de agentes).

ANTECEDENTES

Es determinante ofrecer interoperabilidad a los clientes para desarrollar el uso de los pagos digitales.

La interoperabilidad de plataformas, agentes y clientes son conceptos relacionados pero distintos. La investigación del GCAP sobre el tema resume del siguiente modo estas tres formas distintas de interoperabilidad: interoperabilidad de plataformas, que permite realizar transacciones entre distintos proveedores de servicios; interoperabilidad de agentes, que permite que un solo agente ofrezca servicios prestados por múltiples proveedores; e interoperabilidad de clientes, que permitiría a un cliente acceder a cualquier teléfono en la misma red con una tarjeta SIM y a múltiples cuentas con una misma tarjeta SIM.[20]

5.1 Un enfoque de colaboración

Esta práctica alienta las iniciativas de colaboración e interoperabilidad dirigidas por el sector que beneficien a los clientes. Esto debería hacerse bajo la dirección de supervisores clave, especialmente dadas las preocupaciones sobre las disposiciones

contrarias a la competencia que podrían violar las leyes antimonopolios. Un ejemplo de este enfoque sería la plataforma Bim de dinero móvil recientemente presentada en el Perú. Se trata de una importante iniciativa de colaboración entre el gobierno del Perú, instituciones financieras, operadores de telecomunicaciones y otras partes interesadas. La plataforma permite la interoperabilidad de los servicios financieros digitales en todas las redes celulares y proveedores de pagos así como la de todos sus agentes.[21] Otro ejemplo notable de esta colaboración procede del enfoque de "probar y aprender» utilizado en Tanzania. Para obtener información sobre este último ejemplo, véase el informe de 2016 de la Corporación Financiera Internacional (CFI) titulado *Estudio de caso de Tanzania: Lograr la interoperabilidad en los servicios financieros móviles.*

A diferencia del enfoque originado en el propio sector, las regulaciones gubernamentales pueden prever expresamente la interoperabilidad. Un ejemplo de este enfoque se encuentra en el Reglamento del Sistema Nacional de Pagos de Kenya de 2014, en el que la Regulación 21.1 establece que "un proveedor de servicios de pagos deberá usar sistemas capaces de interoperar con otros sistemas de pagos en el país y en el extranjero". Igualmente, Nigeria exigió la interoperabilidad de los operadores de dinero móvil en 2012.[22]

Otras organizaciones internacionales promueven la interoperabilidad. Tal es el caso de la Guía de *Level One Project* de la Fundación Bill y Melinda Gates, que fomenta la interoperabilidad de las transferencias y el apoyo normativo pertinente;[23] y los principios rectores 3 y 5 del informe PAFI, que piden infraestructura que permita enviar, procesar, compensar y liquidar instrumentos de pago de la misma clase, además de canales de acceso interoperables.

5.2 Obstáculos para la interoperabilidad

También es importante que no haya obstáculos anticompetitivos artificiales que impidan la interoperabilidad. Un ejemplo clásico de este tipo de obstáculos se presenta cuando un proveedor no permite a sus agentes trabajar con otros proveedores. Estos tipos de acuerdos exclusivos pueden causar grandes molestias a los clientes de otros proveedores en determinadas zonas si aquellos no cuentan con fácil acceso a una red de agentes. Otro ejemplo sería un acuerdo bajo el cual los clientes de un proveedor sólo pudieran realizar o recibir pagos de otros clientes del mismo proveedor. Sin embargo, se reconoce que hay que mantener el equilibrio entre la competencia y la necesidad de los proveedores de obtener un retorno de la inversión en innovación.

PRÁCTICA 6: Asumir la responsabilidad de los proveedores de servicios al cliente en toda la cadena de valor

Los clientes depositan confianza en los pagos digitales y los usan si el proveedor asume la responsabilidad de las acciones de los agentes, empleados y proveedores de servicios de terceros en toda la cadena de valor.

ALGUNAS MANERAS DE ASUMIR LA RESPONSABILIDAD POR LOS AGENTES, EMPLEADOS Y PROVEEDORES DE SERVICIOS DE TERCEROS SON:

1. **Responsabilidad:** los proveedores asumen la responsabilidad de las acciones y omisiones de sus agentes, empleados y proveedores de servicios de terceros.
2. **Capacitación y supervisión:** los agentes y empleados, y los proveedores de servicios de terceros, están debidamente capacitados (incluso en las características de los productos y en las responsabilidades normativas) y se les supervisa adecuadamente, incluso en lo relativo a las características del producto, las responsabilidades normativas y la conducta relativa a las cuestiones de género. Además cuentan con los recursos necesarios para prestar servicios de pagos de manera competente y legal.
3. **Datos del proveedor:** los agentes entregan a los clientes el nombre y la información de contacto del proveedor cuando estos abren su cuenta y en cualquier momento en que la soliciten.

ANTECEDENTES

6.1 Responsabilidad

Una característica esencial de un mercado responsable de pagos digitales es que los proveedores asumen la responsabilidad de las acciones y omisiones de sus proveedores de servicios y de sus efectos sobre los clientes. Los agentes son un caso particular, y el término "proveedor de servicios de terceros" incluye a los administradores de redes de agentes. En algunos países esta responsabilidad puede estar incluida en el marco de la ley, pero no es el caso en todos los países, y se trata de una cuestión crucial.

Un ejemplo de un enfoque legislativo puede encontrarse en la Regulación 37 de la Normativa sobre dinero electrónico de Tanzania de 2015, que establece que "un proveedor de servicios de pago es responsable ante sus clientes de la(s) acción(es) y omisiones de sus agentes que tengan lugar en el marco del acuerdo de agencia".

La práctica 3 del GSMA también trata sobre el asunto de la responsabilidad de los agentes, pero no se refiere a empleados ni a proveedores de servicio de terceros. La Reglamentación de Indonesia sobre protección de los consumidores de sistemas de pago constituye otro ejemplo, ya que afirma que un proveedor es responsable ante sus consumidores por las pérdidas derivadas de errores cometidos por la administración y los empleados.[24]

6.2 Capacitación y supervisión

Los clientes también esperarían de manera legítima que un proveedor asuma la responsabilidad de la adecuada formación y supervisión de sus agentes, empleados y proveedores de servicios. Esto incluiría, por ejemplo, servicios de capacitación sobre las características y riesgos de los servicios de pago, el modo de utilizar el servicio, la manera de comunicarse con los clientes, las garantías de seguridad (por ejemplo, en lo referente a PIN), mecanismos de recursos del cliente y prácticas prohibidas (como las relativas a fraude y discriminación). Esto debe incluir por igual una conducta adecuada relativa al género que, por ejemplo, impida que los agentes masculinos toquen las manos de las clientas cuando registren sus huellas digitales con fines de identificación biométrica en la India. En el caso de proveedores de servicios de terceros, podrían imponerse las obligaciones pertinentes mediante el acuerdo con el proveedor de servicios.

6.3 Datos del proveedor

Es más probable que un cliente de servicios de pago entre en contacto primeramente con un agente en vez de con el proveedor o con un empleado del proveedor. No obstante, es importante que el cliente sepa quién es el proveedor, para así determinar si desea o no utilizar ese producto o, si decide usar el producto, para saber a quién dirigir cualquier queja que surja.

PRÁCTICA 7: Proteger los datos de los clientes

La protección de los datos digitales de los clientes se ha convertido en un asunto crecientemente importante debido al volumen, velocidad y variedad de datos que se utilizan para mercadeo y calificación de crédito, y a su vez se debe reconocer que el uso de los datos de los clientes puede aumentar la gama de productos a los que estos pueden tener acceso.

ALGUNAS MANERAS EN LAS QUE SE PUEDEN PROTEGER LOS DATOS PERSONALES DE LOS CLIENTES EN UN ENTORNO DIGITAL A NIVEL BÁSICO SON:

1. **Confidencialidad y seguridad:** se toman medidas razonables para garantizar la confidencialidad y seguridad de los datos pertinentes del cliente en las transacciones de pago digitales. Tales datos incluyen, entre otros, la información de identificación y del contrato; historiales de transacciones; credenciales de seguridad; uso de datos en dispositivos, teléfono celular e internet, y datos de geolocalización. Con el consentimiento expreso e informado de los clientes, se pueden usar y divulgar los datos para fines específicos, tales como la promoción de nuevos servicios.
2. **Historial de auditoría:** se pone a la disposición de los clientes y supervisores un claro historial de auditoría de registros de transacciones.

ANTECEDENTES

7.1 Confidencialidad y seguridad

La protección y privacidad de los datos en el entorno digital fue un riesgo importante que se debatió en el Informe de Resultados del *V Foro sobre finanzas responsables y en el Informe del VI Foro sobre finanzas responsables*. También se reconoce como un asunto normativo primordial en el informe sobre los Principios para una Inclusión Financiera Innovadora del G20 (2010).[25] La práctica 7.1 aborda importantes inquietudes acerca de datos personales de los clientes de pagos digitales. Sin embargo, no pretende tratar todos los posibles problemas de datos. Los temas adicionales no cubiertos por esta práctica podrían incluir: derechos de acceso y rectificación; límites a la recolección y uso de información personal (como en lo relativo al uso de información personal para fines de mercadeo); límites de los períodos de retención de datos, y el requisito de publicar información de la política de privacidad del proveedor. La práctica 7 tampoco aborda el uso de analítica de macrodatos con relación a los servicios de pagos digitales.[26]

Hay diversos ejemplos de principios, normas y códigos (así como de legislación nacional) que proporcionan amplia cobertura de cuestiones relacionadas con la protección de datos. Entre dichos ejemplos se encuentran:

- Principios para una Inclusión Financiera Innovadora del G20 (2010).
- Las prácticas de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 2013.
- La propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, de la Resolución de Madrid.
- Los principios de Windhover sobre identidad, confianza y datos digitales de 2014 del *Institute for Data Driven Design*.
- La práctica 6 de los *Principios de Protección al Cliente* de The Smart Campaign (que también limita el uso de datos al propósito principal de recolección, sujeta a consentimiento).
- La práctica 8 del Código de Conducta del GSMA.

También hay requisitos de protección de datos pertinentes a los servicios financieros digitales a nivel nacional, como es el caso de los de Indonesia y Filipinas, entre otros.[27]

7.2 Historial de auditoría

Un historial de auditoría asegura que los clientes obtengan pruebas de transacciones pasadas. Esto puede ser especialmente útil en el caso de una transacción disputada así como para fines de supervisión (por ejemplo, en la comprobación de si se han cumplido las cláusulas de protección de los fondos de los clientes).

PRÁCTICA 8: Proporcionar recursos a los clientes

Los clientes necesitan tener acceso a un sistema de recursos adecuado para manejar los reclamos relacionados con pagos digitales. Esto es especialmente necesario en caso de quejas sobre productos innovadores y desconocidos ofrecidos a través de canales nuevos, y para clientes que vivan en lugares apartados y tengan poco o ningún contacto directo con los proveedores.

ALGUNOS SISTEMAS DE RECURSOS EFICACES PARA CLIENTES DE PAGOS DIGITALES SON:

1. **Quejas:** los clientes pueden acceder fácilmente a un sistema de quejas transparente, gratuito o de bajo costo y eficiente. Este sistema debe ser accesible para todos, independientemente de las normas culturales, el idioma, la movilidad, etc. Idealmente, el sistema puede alojar a clientes vulnerables (como los clientes con discapacidad). El sistema es accesible por vía telefónica o digital (una página web o un mensaje de texto), o visitando la sede del proveedor.
2. **Disputas:** los clientes también tienen acceso a un servicio de terceros independiente que se ocupa de las disputas con los proveedores en los casos en que el proveedor no haya abordado y resuelto la queja del cliente de manera adecuada. Este sistema de terceros es de fácil acceso (incluso por vía telefónica o digital), transparente, eficiente y gratuito o de bajo costo.
3. **Información sobre sistemas de recursos:** la información sobre los términos y condiciones del sistema de recursos de un proveedor se encuentran en el sitio web del proveedor y en las instalaciones del proveedor y el agente. Además, cuando un cliente hace una denuncia recibe una copia de esta información, que puede entregarse en formato digital.
4. **Datos de las quejas:** los proveedores llevan registros de quejas de los clientes y su respuesta a cada queja. Los reguladores también reciben informes periódicos de los datos de las quejas. Se publican los problemas sistémicos del sector, pero teniendo cuidado de no revelar la identidad de los denunciantes.

ANTECEDENTES

8.1 y 8.2 Quejas y disputas

El Enfoque del GCAP sobre finanzas digitales identificó "sistemas de recursos deficientes" como uno de los siete riesgos más importantes que enfrentan los consumidores. Muchos principios, estándares, códigos y regulaciones nacionales abordan la necesidad de sistemas internos y externos de recursos del consumidor, incluida la práctica 7 del Código de Conducta del GSMA, el principio rector 2 del Informe PAFI y la práctica 7 de los principios de protección al cliente de *The Smart Campaign.*[28]

La práctica 8 procura abordar los sistemas de recursos del cliente de un proveedor, además de los servicios de solución de disputas externas. Ejemplos de esto último son, entre otros, un programa de defensoría financiera del consumidor instituido por el propio sector o por ley, o un servicio de mediación prestado por un supervisor. A nivel nacional, algunas de las entidades de solución de controversias son la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) en México,[29] el nuevo programa del Defensor financiero de Malasia,[30] el Defensor para servicios bancarios en Sudáfrica,[31] y la oficina del Defensor del pueblo en Rwanda.[32]

8.3 Información sobre sistemas de recursos

Los clientes deben saber dónde ir si tienen una queja o una disputa. Por esa razón, la información sobre sistemas de recursos debe ser de fácil acceso. Esto coincide con las conclusiones del reciente *Client Voice Project de The Smart Campaign,* que reveló una falta

generalizada de conciencia sobre canales de recursos en los cuatro países en que se aplicaron encuestas (Benín, Georgia, Pakistán y el Perú). El Perú y Georgia parecen contar con un sólido marco de protección del consumidor.[33] En Benín sólo el 14 por ciento de los encuestados recordó que se les informara dónde acudir si tenían problemas o quejas. En Georgia, Pakistán y el Perú ese porcentaje alcanzó el 37, 34 y 29 por ciento respectivamente.[34]

Los *Estándares de Certificación en Protección al Cliente* de *The Smart Campaign* ahora exigen que "la entidad financiera informe a los clientes sobre su derecho a reclamar y cómo presentar una queja".[35]

8.4 Datos de las quejas

Desde la perspectiva de los clientes, es importante que los proveedores lleven un registro del progreso de cada queja y del resultado final. Lo ideal sería que los datos de las quejas también se informaran al regulador correspondiente, para que éste identifique posibles problemas sistémicos que afecten a los clientes. Dicha información debe publicarse para que sea útil para los clientes.

La práctica 8.4 no dispone que se publique la identidad de los proveedores cuando se haga pública la información sobre las quejas sistémicas. No obstante, dichos datos pueden ayudar no sólo a los consumidores que buscan elegir un proveedor, sino también a los mismos proveedores, ya que les permite hacer comparaciones con la competencia. El supervisor o un servicio de defensoría financiera podrían proporcionar esta información. Algunos ejemplos de estas modalidades son la base de datos de reclamaciones con que cuenta la Dirección de Protección Financiera del Consumidor de Estados Unidos;[36] los datos de la autoridad financiera del Reino Unido sobre empresas individuales;[37] y la información publicada por el Buró de entidades financieras de México.[38]

Glosario de términos y siglas

AML/CTF	Siglas en inglés de medidas de prevención del lavado de activos y del financiamiento del terrorismo e inclusión financiera
Código de Pagos Electrónicos de Australia	Código de pagos electrónicos administrado por la Comisión Australiana de Valores e Inversiones
GCAP	Grupo consultivo de ayuda a la población más pobre
Enfoque del GCAP sobre Finanzas Digitales	*Recomendaciones del Grupo de Acción Financiera Internacional (GAFI): Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y de la proliferación (2012)*
GAFI	Grupo de Acción Financiera Internacional
Recomendaciones del GAFI	Recomendaciones del *Grupo de Acción Financiera Internacional (GAFI):* Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y de la proliferación (2012)
Guía de Level One Project de la Fundación Gates	Guía de *Level One Project* de la Fundación Bill y Melinda Gates: Diseño de un nuevo sistema para la inclusión financiera (2015)
GSMA	Sistema global para las comunicaciones móviles
Código de Conducta del GSMA	El Código de Conducta del GSMA para proveedores de dinero móvil (2014)
Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago	Reglamentación Número 16/1/PBI/2014 del Banco de Indonesia
CFI	Corporación Financiera Internacional
OCDE	Organización de Cooperación y Desarrollo Económicos
Informe PAFI	Aspectos de Pagos de la Inclusión Financiera (PAFI), un informe del comité de pagos e infraestructura de mercado del Banco de Pagos Internacionales y el Banco Mundial (2016)
PSD2	Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo del 25 de noviembre de 2015 sobre Servicios de pago en el mercado
Informe de Resultados del V Foro sobre Finanzas Responsables	V Foro sobre finanzas responsables: Informe de resultados sobre las finanzas digitales responsables (2014)
VI Foro sobre Finanzas Responsables	VI Foro sobre finanzas responsables: Informe sobre evidencia einnovación para ampliar las finanzas digitales inclusivas (2015)
Los Estándares de Certificación de *The Smart Campaign*	Los estándares de certificación en protección al cliente de *The Smart Campaign* (2016)
Normativa sobre Dinero Electrónico de Tanzania	Normativa sobre dinero electrónico de Tanzania (2015)

Referencias

Afghanistan Da Afghanistan Bank Law (2003)
http://dab.gov.af/Content/Media/Documents/DABLaw21102015144197075533325325.pdf

Afghanistan Mobile Service Providers Regulation
http://www.fintraca.gov.af/assets/pdf/money_service_providers_regulation.pdf

Australia ePayments Code (2016)
http://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf

Bank Indonesia Regulation (2014) No. 16 /1/PBI Consumer Protection in Payment System Service
http://www.bi.go.id/en/peraturan/sistem-pembayaran/Documents/pbi_160114.pdf

Centre for Financial Inclusion (2016) 'BiM The First Fully - Interoperable Mobile Money Platform: Now Live in Peru'
https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru/

Consumer Financial Protection Bureau, (2016) 'Consumer Complaints Database'
http://www.consumerfinance.gov/data-research/consumer-complaints/

CGAP (2015) 'Doing Digital Finance Right'
http://www.cgap.org/publications/doing-digital-finance-right

CGAP (2016) 'Interoperability in Branchless Banking and Mobile Money'
http://www.cgap.org/blog/interoperability-branchless-banking-and-mobile-money-0

Committee for Payments and Markets Infrastructure of the Bank for International Settlements and the World Bank Group (2016)
'Payments Aspects of Financial Inclusion Report'
http://pubdocs.worldbank.org/pubdocs/publicdoc/2016/4/963011459859364335/payment-systems-PAFI-Report2016.pdf

Financial Action Task Force (2012) 'International Standards on Combating Money Laundering and the Financing of Terrorism & Protection'
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Financial Conduct Authority (United Kingdom) (2016) 'Complaints Data'
https://www.the-fca.org.uk/firms/complaints-data

G20 (2011) 'High-Level Principles on Financial Consumer Protection'
https://www.oecd.org/daf/fin/financial-markets/48892010.pdf

G20 Global Partnership for Financial Inclusion (2016) 'Global Standard-Setting Bodies Financial Inclusion The Evolving Landscape'
http://www.gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-evolving-landscape

G20 Principles for Innovative Financial Inclusion (2010). Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group. https://www.gpfi.org/sites/default/files/documents/Principles%20and%20Report%20on%20Innovative%20Financial%20Inclusion_0.pdf

J Greenacre and RP Buckley, University of New South Wales (2014) 'Using Trusts to Protect Mobile Money Customers'
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454

GSMA (2014) 'Code of Conduct for Mobile Money Providers'
http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/policy-and-regulation/code-of-conduct

IFC (2016) 'Tanzania Case Study Achieving Interoperability in Mobile Financial Services'
http://www.ifc.org/wps/wcm/connect/8d518d004799ebf1bb8fff299ede9589/IFC+Tanzania+Case+study+10_03_2015.pdf?MOD=AJPERES

International Conference of Data Protection and Privacy Commissioners (2009)
'Madrid Resolution International Standards on the Protection of Personal Data and Privacy'
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

Kenya The National Payment System Act, 2011 (No. 39 of 2011)
https://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf

Kenya The National Payment System Regulations (2014)
https://www.centralbank.go.ke/images/docs/legislation/NPSRegulations2014.pdf

Malawi Mobile Payments Guidelines (2011)
https://www.rbm.mw/PaymentSystems/

Nigeria Consumer Protection Framework (2016) https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf

Nigeria (2012) Central Bank of Nigeria Direction BPS/DIR/GEN/CIR/01/014
http://www.cenbank.org/out/2012/ccd/timeline%20for%20interoperability%20&%20interconnectivity.pdf

OECD (2013) 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Philippines Central Bank E-Money Circular 649 (2009)
http://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf

Responsible Finance Forum V (2014) 'Responsible Digital Finance Outcomes Report'
https://www.responsiblefinanceforum.org/wp-content/uploads/RFFVSummaryRepor.pdf

Responsible Finance Forum VI (2015) 'Evidence and Innovation for Scaling Inclusive Digital Finance Report'
https://responsiblefinanceforum.org/wp-content/uploads/RFF6-report-5_21-final-low_res.pdf

Tanzania The National Payments System Act (2015)
https://www.bot-tz.org/PaymentSystem/NPS%20Act%202015.pdf

Tanzania The Electronic Money Regulations (2015)
https://www.bot-tz.org/PaymentSystem/GN-THE%20ELECTRONIC%20MONEY%20REGULATIONS%202015.pdf

The Bill and Melinda Gates Foundation (2015) 'Level One Project Guide: Designing a New System for Financial Inclusion'
https://www.betterthancash.org/tools-research/resources/the-level-one-project-guide-designing-a-new-system-for-financial-inclusion

The Smart Campaign (2011) 'The Client Protection Principles'
http://www.smartcampaign.org/about/smart-microfinance-and-the-client-protection-principles

The Smart Campaign (2015) 'My Turn to Speak: Voices of Microfinance Clients in Benin, Pakistan, Peru and Georgia'
http://smartcampaign.org/storage/documents/Synthesis_Report_ENG_FINAL.pdf

The Smart Campaign (2016) 'The Client Protection Certification Standards'
http://www.smartcampaign.org/storage/documents/Standards_2.0_English_Final.pdf

ID3 (2014) 'The Windhover Principles for Digital Identity, Trust, and Data'
https://idcubed.org/about/vision-mission-2/

World Bank (2012) 'Good Practices on Financial Consumer Protection'
http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf

Notas finales

1. La Alianza Better Than Cash, Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services, (se publicará en agosto de 2016).
2. Véase, por ejemplo, el informe *Payments Aspects of Financial Inclusion* (PAFI) del Comité de Pagos e Infraestructura de Mercados y el Banco Mundial; el informe *Good Practices for Financial Consumer Protection, del Banco Mundial; los Client Protection Principles* de The Smart Campaign; *Level One Project Guide: Designing a New System for Financial Inclusion,* De la Fundación Bill y Melinda Gates; el informe *Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape* de la Alianza Mundial para la Inclusión Financiera del G20, de 2016; y el *Código de Conducta del GSMA* para Proveedores de Dinero Móvil.
3. A modo de ejemplo, véase la Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago, que identifica como primer principio de protección del cliente el «trato justo y equitativo» (Artículo 3a). Un segundo ejemplo aparece en el Principio 5 de los Principios de Protección del Cliente de The Smart Campaign, que exigen un trato justo y respetuoso para los clientes.
4. Artículo 8 de la Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago.
5. Véase la Recomendación 10 en las *Recomendaciones del Grupo de Acción Financiera (GAFI): Estándares Internacionales sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y de la Proliferación* (2012), que exige (entre otras cosas) que las medidas de diligencia debida relativas al cliente comprendan: "Identificar al cliente y comprobar su identidad mediante documentos, datos o información confiable de fuentes independientes", y que las instituciones financieras "determinen el alcance de dichas medidas a partir de un enfoque basado en riesgos, según las Notas de Interpretación de esta Recomendación y de la Recomendación 1". En resumen, las Notas de Interpretación de la Recomendación 1 plantean que se podrían usar medidas simplificadas para identificar, evaluar, monitorear, gestionar y mitigar los riesgos del lavado de activos y el financiamiento del terrorismo allí donde los riesgos sean escasos. Cabe destacar que todas las prácticas propuestas están sujetas a las leyes pertinentes, incluidas las leyes contra el lavado de activos y contra el financiamiento del terrorismo. Además, las Notas de Interpretación de la Recomendación 10 describen situaciones de bajo riesgo como aquellas en que estén en juego "Productos o servicios financieros que ofrecen prestaciones adecuadamente definidas y limitadas a ciertos tipos de clientes con el fin de aumentar el acceso para fines de inclusión financiera". Del mismo modo, la Directriz 2.5.1 del *Código de Conducta del Groupe Spéciale Mobile Association (GSMA) para Proveedores de Dinero Móvil* (en adelante, *Código de Conducta del GSMA)* establece que los proveedores "podrían utilizar un enfoque basado en los riesgos ['conocer al cliente'] si lo permiten las leyes y regulaciones locales".
6. *Directriz del GAFI: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion [Medidas de Prevención del Lavado de Activos y del Financiamiento del Terrorismo e Inclusión Financiera],* (2012), Párrafo 67.
7. Capítulo C del Código de Pagos Electrónicos de Australia.
8. El *Enfoque del GCAP sobre Finanzas Digitales* contiene conclusiones de investigación sobre los consumidores realizadas en 16 mercados: Bangladesh, Colombia, Cote d'Ivoire, Ghana, Haití, Kenya, India, Indonesia, Nigeria, Pakistán, Perú, Filipinas, Rusia, Rwanda, Tanzania y Uganda. Asimismo, presenta conclusiones de un estudio inicial sobre las acciones pertinentes a la mitigación de riesgos realizadas por los proveedores de servicios, así como las medidas de regulación y supervisión observadas referentes a la protección del consumidor.
9. Cláusulas 14.2 y 14.3 del Código de Pagos Electrónicos de Australia.
10. Greenacre and Buckley, *Using Trusts to Protect Mobile Money Customers,* (2014). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454
11. Reglamentación de Proveedores de Servicios Móviles y Ley Bancaria de Afganistán; Ley del Sistema Nacional de Pagos de Kenya, de 2011 (N.º 39 de 2011) y la Reglamentación del Sistema Nacional de Pagos, de 2014; las Directrices para Sistema de Pagos Móviles de Malawi; la Circular 649 sobre Dinero Electrónico del Banco Central de Filipinas, de 2009; la Ley del Sistema Nacional de Pagos de Tanzania, de 2015 y las Regulaciones sobre Dinero Electrónico, de 2015.
12. La Sección 4(H) de la Circular 649 sobre Dinero Electrónico del Banco Central de Filipinas, de 2009.
13. Los Artículos 3(c) y 14(2)(c) de la Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago.
14. Marco de Protección al Consumidor de Nigeria 2016, sección 2.1.6.(2)
15. Párrafo 95 de la PSD2.
16. Ibíd., véanse los Artículos 71–74 y la definición de "sólida autenticación del cliente" en el Artículo 4.
17. Ibíd., Artículo 72.
18. http://www.buro.gob.mx/inicio.php?id_sector=0
19. Véase, por ejemplo, "Evidence Spotlight: How Commitment Products Break Down Behavioral Barriers to Savings," página 7 del Informe del VI *Foro sobre Finanzas Responsables.*
20. Enfoque del GCAP sobre Finanzas Digitales.
21. https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru
22. Directiva BPS/DIR/GEN/CIR/01/014 del Banco Central de Nigeria, de 2012
23. Páginas 4 y 8 de la *Guía de Level One Project de la Fundación Bill y Melinda Gates.*
24. Artículo 10 de la Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago.
25. Principios e informes sobre inclusión financiera innovadora del subgrupo de acceso a través de la innovación del Grupos de Expertos en Inclusión Financiera del G20, página 13.
26. "Macrodatos" se define de muchas maneras distintas, pero una definición de uso común es la de Gartner: "Macrodatos" son activos informáticos de alto volumen, alta velocidad y amplia variedad que exigen formas innovadoras y económicas de procesamiento de información a fin de permitir un mejor conocimiento y toma de decisiones" (consulte el Gartner IT Glossary, disponible en inglés en http://www.gartner.com/it- glossary/big-data).
27. Véanse la Sección 4(H) de la Circular 649 sobre Dinero Electrónico del Banco Central de Filipinas y los Artículos 3(c), 14 y 15 de la Reglamentación de Indonesia sobre Protección de los Consumidores de Sistemas de Pago, de 2014.
28. Un ejemplo de nivel nacional de un requisito de programa de quejas interno se encuentra en la sección 4(F) de la Circular 649 sobre Dinero Electrónico del Banco Central de Filipinas, que exige que los emisores de dinero electrónico cuenten con un mecanismo de compensación aceptable para el manejo de las quejas de los consumidores. La sección 4(G) también exige que se entregue a los consumidores la información sobre procedimientos de compensación. Otro ejemplo son las disposiciones sobre compensación de los consumidores presentes en la Regulación 45 de la Normativa sobre Dinero Electrónico de Tanzania, de 2015.
29. http://www.condusef.gob.mx/index.php/english
30. http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press_all&ac=3283
31. http://www.obssa.co.za/
32. http://ombudsman.gov.rw/
33. The Smart Campaign, My Turn to Speak: Voices of Microfinance Clients in Benin, Pakistan, Peru and Georgia' [Me toca a mí hablar: Voces de clientes de microfinanzas en Benín, Pakistán, Perú y Georgia], de 2015.
34. Ibíd., Figura 27.
35. Principio 7, Estándar 2.
36. http://www.consumerfinance.gov/complaintdatabase/
37. http://www.fca.org.uk/firms/systems-reporting/complaints-data
38. http://www.buro.gob.mx/inicio.php?id_sector=0

WWW.BETTERTHANCASH.ORG

Acerca de la Alianza Better Than Cash

La Alianza Better Than Cash es una asociación de gobiernos, empresas, y organizaciones internacionales que acelera la transición de pagos en efectivo a pagos digitales para contribuir a la reducción de la pobreza e impulsar el crecimiento inclusivo. Con base en las Naciones Unidas, la Alianza tiene más de 50 miembros, trabaja en estrecha colaboración con otras organizaciones a nivel mundial, y es un asociado en la ejecución de la Alianza Mundial para la Inclusión Financiera del G-20.