Mobile Money for the Unbanked

Gestionando el Riesgo de Fraude en el Dinero Móvil

Autores: Lara Gilman y Michael Joyce

Resumen ejecutivo

La gestión de riesgos es un componente clave para el éxito comercial de cualquier negocio. Una gestión de riesgos efectiva constituye la base para un crecimiento comercial sostenible porque protege dos activos comerciales clave: la reputación y los ingresos.

Los operadores móviles están familiarizados con la gestión de riesgos por el lado de los negocios GSM y aquellos que han lanzado el dinero móvil son conscientes de que éste acarrea diferentes clases de riesgo – particularmente el riesgo de fraude. Este documento presenta una estructura para manejar el fraude y el riesgo. Los cuatro elementos clave de esa estructura son: (i) determinar el apetito de riesgo, (ii) identificar y evaluar los riesgos; (iii) establecer controles efectivos; y (iv) monitorear y revisar la estrategia del manejo del riesgo.

En nuestra investigación, Dinero Móvil para los No Bancarizados (MMU por sus siglas en inglés) halló que los operadores son conscientes de la necesidad de desarrollar una sólida estrategia para la gestión de riesgo del dinero móvil. Este documento destacará algunas prácticas efectivas que los operadores utilizan para manejar el riesgo de fraude, a fin de ayudar a los proveedores de dinero móvil mientras continúan revisando y mejorando sus estrategias para la gestión de riesgo.

Introducción

Gestión de riesgo en el dinero móvil es una tarea que constituye un desafío, especialmente cuando se trata del riesgo de fraude. El fraude no solamente tiene como resultado pérdidas económicas para los clientes o para un proveedor de dinero móvil, sino que también daña la reputación del servicio al cliente y pone en peligro la reputación de la industria en general. Como tal, mitigar el riesgo de fraude constituye un objetivo fundamental en una sólida estrategia para el manejo del riesgo.

En la práctica, los operadores móviles, bancos y las terceras partes reconocen que la gestión de riesgo es un pilar esencial para el éxito comercial sostenible de un servicio de dinero móvil. Tal como lo abordara MMU en otras publicaciones, el dinero móvil es cualquier cosa menos un servicio rápido y con fácil valor agregado (VAS por sus siglas en inglés). Los operadores con estrategias efectivas para la gestión de riesgo son conscientes de la complicada naturaleza del dinero móvil y han invertido dedicados recursos para manejar las actividades de fraude y de garantía de ingresos.

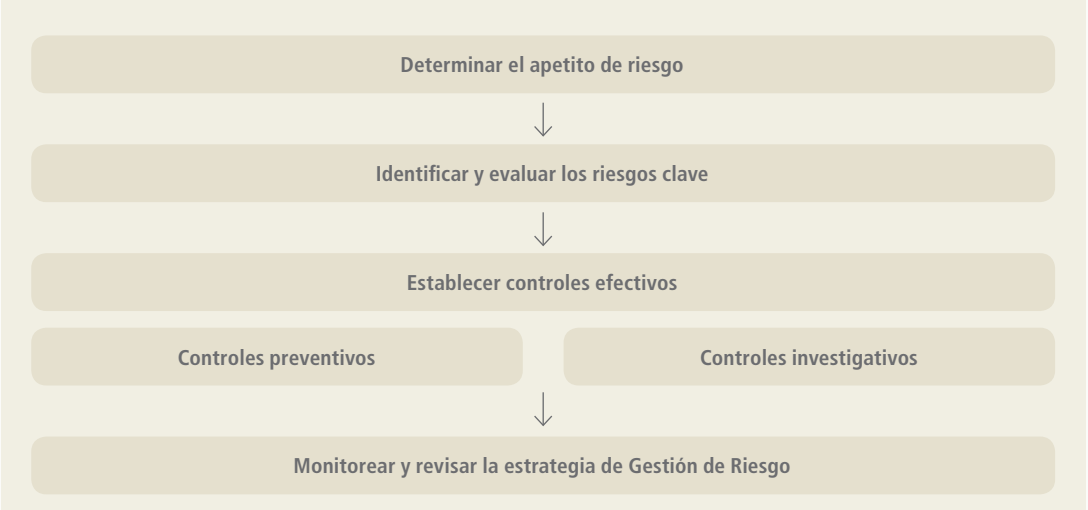
Sin embargo, las estrategias específicas para la gestión de riesgo varían de operador a operador. Las estrategias se ven influidas por numerosos factores, incluyendo la etapa de desarrollo, la estructura organizacional, el número de productos en oferta, el entorno regulatorio y el contexto del mercado local.

Aunque la estructura del manejo del fraude puede diferir, hay una estructura común con la que se está ampliamente de acuerdo en cuanto a que está totalmente aceptada como el fundamento de cualquier estrategia para la gestión de riesgo del dinero móvil. La estructura está compuesta de cuatro elementos que los servicios de dinero móvil utilizan para manejar el riesgo: determinar el apetito de riesgo, identificar los riesgos, establecer controles y monitorear la efectividad. El siguiente diagrama es una representación visual de la estructura y es una guía para los temas cubiertos en este documento.

Esta estructura para la gestión de riesgo no está lejos de los estándares de ISO 31000:2009[1] o de SOX[2], que son alineamientos globales acerca de la gestión de riesgo. Como tales, pueden aplicarse a muchas industrias pero nuestro enfoque se dirige hacia cómo se utiliza en el contexto del dinero móvil, a fin de destacar cómo los operadores mitigan el riesgo de fraude en el dinero móvil. Otros escollos incluyen el cumplimiento, la continuidad del negocio, salud y seguridad y robo físico, pero éstos están más allá del alcance y no serán abordados específicamente en este documento.

Determinar el apetito de riesgo: el fundamento de la gestión de riesgo

Para dar prioridad y controlar exitosamente el riesgo de fraude, los operadores de dinero móvil necesitan entender su apetito respecto al riesgo, lo que es un modo de expresar cuáles son los costos que confortablemente podrían asumir. Cada riesgo tendrá un costo, así como cada control. Un servicio de dinero móvil que es más conservador puede inclinarse por evitar el riesgo y estar más dispuesto a aceptar un crecimiento más lento o costos operacionales más



1 ISO Standard 31000:2009 (Gestión de riesgos- principios y directrices) fue consultada en la elaboración de este documento, pero el marco presentado aquí difiere en varios aspectos. Los gestores del riesgo que desarrollan documentación sobre el riesgo y los marcos para su organización, deberían considerar cualquier requerimiento regulatorio local así como las normas internacionales como la ISO 31000.

2 US Sarbanes-Oxley Act 2002, una norma de los Estado Unidos sobre responsabilidad financiera.

elevados. Alternativamente, un servicio que está más enfocado en una rápida expansión e innovación estará más abierto a aceptar una mayor exposición al riesgo. Lo importante es que los gerentes del dinero móvil y aquellos responsables por el crecimiento comercial tengan una guía acerca de los niveles apropiados del riesgo, cuando desarrollan estrategias comerciales o exploran la oferta de nuevos servicios.

De la misma manera que el apetito por el riesgo en los servicios de dinero móvil puede variar, también pueden hacerlo las metodologías utilizadas para determinar el apetito de riesgo. Algunos operadores pueden intentar definir un apetito cuantitativo por el riesgo (por ejemplo, para que menos de un cierto porcentaje de transacciones estén sujetas a fraudes o quejas). Otros pueden utilizar una escala cualitativa, tal como definir los niveles de apetito por el riesgo como adversos, minimalistas, cautelosos, abiertos o hambrientos.[3]

El apoyo para el desarrollo del apetito por el riesgo podría tener su origen en un número de actores. Hemos visto algunos servicios que confían en sus asociados bancarios para una guía del nivel apropiado de apetito acorde al riesgo. Otros servicios utilizan mayormente el apoyo a nivel de grupo, mientras que algunos servicios desarrollan apetito de riesgo mediante el equipo de fraude y de garantía de ingresos que maneja los negocios GSM. Aunque que este paso en el proceso puede ser de alguna manera conceptual, es muy importante a fin de estar en una posición que permita crear controles efectivos y relevantes.

Identificar y evaluar los riesgos clave: comprendiendo el potencial del fraude

Grupo Orange: Los primeros pasos para manejar el riesgo en el dinero móvil

Antes del lanzamiento del Orange Money, el Grupo Orange sabía que ellos tenían que mirar a este nuevo servicio con una mirada fresca. Mientras los equipos comerciales y de mercadeo evaluaban los beneficios potenciales directos e indirectos en cuanto a lanzar el dinero móvil, el equipo de fraude corporativo y garantía de ingresos necesitaba identificar y evaluar los riesgos de un servicio nuevo y complicado. Para Orange, el objetivo más importante era proteger del fraude los intereses de los clientes de Orange Money y a la vez asegurar que el servicio permanecía accesible y fácilmente utilizable. Orange reconoció que una sólida estrategia para la gestión de riesgo sería fundamental para desarrollar la confianza entre los clientes.

El primer paso del equipo para comprender cómo manejar los riesgos en el dinero móvil fue analizar las vulnerabilidades del servicio. Además de confiar en la riqueza de su propia experiencia, proveniente de los negocios GSM, el equipo de fraude buscó el apoyo de expertos externos y de industrias comparables, tales como otros servicios financieros y de pagos. Para elaborar una cartera de fraudes potenciales, Orange estaba mejor equipada para desarrollar procesos y umbrales destinados a mitigar los riesgos del dinero móvil.

El beneficio de crear una estrategia a partir de cero es que permite al operador adecuar esa estrategia a los requerimientos del servicio. El dinero móvil es inherentemente complicado, requiriendo controles y procesos que van más allá de los negocios de GSM. Para cada nuevo servicio, la perspectiva de elaborar una estrategia partiendo de cero puede parecer lenta, pero es necesaria. El primer paso para elaborar esa estrategia consiste en identificar y comprender las vulnerabilidades en el servicio de dinero móvil.

A fin de crear una estrategia efectiva para la gestión de riesgo, los operadores necesitan identificar las vulnerabilidades en las operaciones de su servicio. El proceso de identificación del riesgo a menudo es realizado por aquellos responsables de la gestión de riesgo del negocio en general, tal como un equipo de garantía de los ingresos. Por ejemplo, hemos visto al menos un par de operadores móviles que han creado un proceso de revisión para cada nuevo producto en sus servicios de dinero móvil. Como parte de la revisión, cada nuevo producto o precio debe ser revisado por todas las partes interesadas en el negocio, incluyendo ventas, mercadeo, distribución, finanzas y seguridad y garantía de ingresos. Los equipos de seguridad y de garantía de ingresos identifican y evalúan la probabilidad de riesgos y estiman su impacto. Aunque éste no es el único modelo en la industria, es importante destacar que la responsabilidad para identificar los riesgos ha sido claramente asignada a un equipo específico.

Por lo tanto, ¿en dónde se hallan algunos de los riesgos clave de fraude en el dinero móvil?

Hay riesgos que existen en cada servicio de dinero móvil alrededor del mundo, tales como el potencial robo de la información del cliente o la manipulación en la conciliación de balances de dinero electrónico. Sin embargo, puesto que la actividad fraudulenta varía de un servicio a otro, es más relevante observar la identificación del riesgo desde la perspectiva del ecosistema de pagos. En otras palabras, ¿dónde en el proceso de dinero móvil podrían los actores o participantes estar en riesgo o tener capacidad para cometer fraude? Los actores clave que deben ser considerados son los clientes (riesgo de transacciones), el agente (riesgo de canal) y el empleado (riesgo interno).

3 "Pensando acerca del riesgo: manejando su apetito del riesgo: la guía de un profesional" HM Treasury, Noviembre 2006

Fraudes potenciales en Dinero Móvil		
Transaccional	Canal	Interno
■ **Vishing/Smishing:** uso de llamadas telefónicas o mensajes de texto para obtener datos personales como números de cuenta, PIN o detalles de identificación personal. ■ **Estafa de pago anticipado:** clientes que son timados y envían dinero en medio de falsas promesas o circunstancias. ■ **Fraude de sueldo:** empleados inexistentes o fantasmas que reciben fondos. ■ **Solicitud de devolución:** clientes que reclaman una devolución incluso cuando la transacción ha sido exitosa. ■ **Transacciones falsas:** enviar SMS falsos para hacerles creer a los clientes que una transacción ha sido exitosa, usualmente acompañado de un pedido de retorno.	■ **Transacciones divididas:** agentes dividiendo el efectivo de las transacciones para ganar comisiones múltiples –sólo aplica en las estructuras con comisiones. ■ **Transacciones falsas:** agentes que transfieren fondos de un cliente a su cuenta personal. ■ **Registro de fraude:** creación de cuentas de clientes falsos, inválidos o duplicados con el propósito de obtener comisiones extra por registro.	■ **Fraude interno:** empleados complotando para obtener ganancias financieras injustas. ■ **Robo de identidad:** empleados que, sin autorización, acceden y abusan de la información de los clientes.

Observando a cada actor, los operadores pueden identificar y evaluar las vulnerabilidades en el sistema. Por ejemplo, a menudo los clientes son las víctimas del fraude porque no tienen su PIN adecuadamente protegido. Dentro del canal, los agentes podrían explotar el sistema dividiendo las transacciones para obtener una ganancia indebida. Aunque esto no podría describirse como fraude en un sentido legal, los operadores a menudo tratan esto como un fraude puesto que tiene el mismo efecto para la línea de ingresos de los negocios. Es fundamental comprender el riesgo interno, o el riesgo de que un empleado defraude a la compañía, porque la exposición financiera y de reputación puede ser muy grande, aún cuando la probabilidad pueda ser baja. Los servicios de dinero móvil con efectivas estrategias para la gestión de riesgo, han sido meticulosos en la revisión de cualquiera de las vulnerabilidades, especialmente el proceso de conciliación del dinero electrónico, que podría permitir a los empleados defraudar a la compañía. Identificar el riesgo de fraude desde la perspectiva de todas las partes interesadas involucradas, proporciona al operador de dinero móvil una comprensión de principio a fin de los riesgos que deben ser manejados.

Una vez que los riesgos han sido identificados, deben ser comparados con el apetito de riesgo establecido. Cualquier riesgo que caiga fuera del apetito de riesgo de la compañía, necesitará una mayor investigación y se tendrán que establecer controles para manejar o reducir estos riesgos hasta que sean aceptables para el negocio.

Aspectos a considerar cuando se identifican y evalúan los riesgos operacionales en dinero móvil

- ¿Cuáles son las partes más complejas del proceso?
- ¿Hay algunas transacciones de mucho valor, y elevado riesgo que tienen lugar regularmente?
- ¿Existen mecanismos de autenticación que puedan ser falsificados fácilmente?
- ¿Cómo podría alguien abusar del sistema?
- ¿Cómo podría alguien interrumpir las operaciones?
- ¿Cuáles son los fraudes que prevalecen en el país además del dinero móvil? ¿Cuán comunes son?
- ¿Cuál es el nivel general de actividad criminal y la fortaleza de los cuerpos policiales en el país?
- ¿Cuál es la posibilidad del riesgo?
- ¿Cuál es el impacto potencial sobre los negocios (financieramente y de reputación)?

Establecer controles efectivos: mitigando el riesgo de fraude

Con los riesgos clave identificados, el siguiente paso para el operador de dinero móvil consiste en establecer controles efectivos, siendo ésta una acción o política efectiva en cuanto a los costos para gestionar riesgos específicos. Un control exitoso apoyará, pero no bloqueará, un crecimiento comercial sostenible.

Utilizando controles para mitigar el riesgo en el dinero móvil

Los controles en el dinero móvil son ya sea preventivos, lo que reduce la posibilidad de actividades fraudulentas, o investigativos, que monitorean e informan acerca de tendencias o actividades que ya han sucedido. En la Tabla 1 hemos esbozado los controles clave puesto que afectan a la mayoría de los servicios de dinero móvil.

Aunque ésta no es una lista completa, cada uno de estos controles aborda por lo menos un riesgo específico asociado con el dinero móvil. Por ejemplo, los sistemas de control de acceso ayudan a reducir el riesgo de robo de la información del cliente, mientras que el monitoreo y el análisis de transacciones sospechosas incrementa la visibilidad de una actividad fraudulenta.

Tabla 1: Ejemplos de control en dinero móvil

Controles Preventivos	Controles Investigativos
■ Control de acceso para proteger la información de los clientes.	■ Monitorear y analizar actividades sopechosas.
■ Separación de tareas para reducir error o fraude en procedimientos de alto riesgo (por ej. conciliación de saldos de dinero electrónico)	■ Monitorear la actividad de acceso al sistema.
■ Umbrales para a mitigar los riesgos asociados con el lavado de dinero y el terrorismo económico (AML/CFT por sus siglas en inglés)	■ Crear procedimientos de recurso y escalamientos robustos para los problemas con los clientes.
■ Campañas de concientización para incrementar la educación y protección del cliente.	■ Monitorear la actividad de los agentes.
■ Capacitación de agentes en prácticas aceptables y los términos y condiciones.	■ Alertas SMS a los clientes
■ Entrenar a los empleados en sus roles y responsabilidades.	■ Manejo de revisiones de transacciones de alto valor.

Los controles preventivos son generalmente considerados como más sólidos que los controles investigativos, especialmente si estos controles pueden ser implementados como características técnicas del sistema de dinero móvil. Si controles tales como la separación de tareas, los derechos de acceso o si se ha desplegado un endurecimiento de la red, es importante que estos controles sean implementados sólidamente, con la documentación apropiada, revisada y puesta a prueba. Si los controles están establecidos pero son fácilmente burlados (por ejemplo, si la separación de tareas está establecida, pero los usuarios comúnmente comparten contraseñas para evitarla o sortearla), aún permanecen los riesgos de fraude.

El tamaño del servicio y la disponibilidad de recursos pueden tener un impacto en cuanto a si un servicio confía más en controles preventivos o de investigación.

Easypaisa de Telenor Pakistán: Utilizando controles para manejar el arbitraje de los agentes

Los modelos de comisiones escalonadas permiten a los agentes obtener mayores beneficios a partir de transacciones de bajo valor, lo que es crítico en los programas de dinero móvil en donde las transacciones de bajo valor impulsan los negocios. Easypaisa decidió seguir un modelo de precios en niveles para aprovechar estos beneficios comerciales. Sin embargo, los modelos de comisión en niveles son inherentemente más riesgosos que los modelos basados en porcentajes, con más oportunidades para los agentes de abusar del sistema, separando las transacciones para obtener múltiples comisiones.

Más que abandonar los beneficios del modelo de comisiones en niveles, Easypaisa implementó un control preventivo e investigativo para mitigar el riesgo. Ambos controles requirieron que Easypaisa realizara análisis acerca de la actividad de los clientes. Ellos descubrieron dos hechos que ayudaron a crear controles adecuados a los requisitos específicos de su servicio. Primeramente, la conducta normal del cliente consistía en depositar al menos 50 rupias en su cuenta de Easypaisa cada vez. En segundo lugar, el equipo determinó que en un periodo de 15 días, cualquier cuenta que recibiera más de 45 depósitos de efectivo (promedio de tres depósitos por día) era anormal y a menudo vinculada a una actividad sospechosa.

La identificación de una conducta "normal" versus "anormal" significó que el equipo de Easypaisa podía crear controles que podrían ser efectivos pero no excesivos. Saber que los clientes depositan al menos 50 rupias significó que Easypaisa podía crear un depósito mínimo que no perjudicaría la experiencia del cliente, pero haría más difícil para los agentes dividir las transacciones. De igual manera, comprendiendo los patrones de una conducta "anormal", Easypaisa podría desarrollar un control investigativo en donde ellos crearon informes para destacar cualquier cuenta recibiendo más de 45 depósitos de efectivo en el mismo punto de agente, en un período de 15 días. Mediante la creación de estos controles, Easypaisa pudo obtener ventaja de los beneficios comerciales de las comisiones en niveles, manejando a la vez su nivel de exposición al riesgo.

Herramientas para asegurar controles exitosos: información, comunicación y procedimientos internos claramente definidos

Existen tres herramientas que los programas de dinero móvil utilizan a fin de implementar controles de manera efectiva:

1) Datos confiables y relevantes y paneles de control.

2) Canales transparentes de reporte y comunicación entre las partes interesadas, incluyendo a los clientes.

3) Procedimientos internos que definen cómo elevar la conciencia y la acción ante la detección de actividades sospechosas.

La información constituye un activo muy importante cuando se trata de manejar y monitorear el fraude en el dinero móvil. El monitoreo de la actividad transaccional es un punto de referencia clave en una estrategia efectiva, pero no existe un único panel de control que pudiera ser adoptado por todos los programas de dinero móvil. La información confiable proviene del trabajo realizado con los equipos administrativos o los proveedores de la plataforma. Mirando nuevamente cómo Easypaisa maneja el arbitraje de agentes, ellos necesitaban poner al descubierto hechos localmente relevantes que podrían utilizar para determinar una conducta normal o anormal.

Safaricom M-PESA: Comunicación como un control preventivo – una mirada a la concientización del cliente

Una de las principales prioridades para M-PESA de Safaricom es mitigar el riesgo de estafas en contra de los clientes. En vez de intentar utilizar solamente controles de investigación, Safaricom confía plenamente en un control preventivo para reducir los riesgos de estafas contra los clientes. Safaricom ha hallado que el control preventivo más efectivo consiste en elevar el conocimiento del cliente a través de una clara comunicación. Para llegar a los clientes de M-PESA, Safaricom utiliza un enfoque con múltiples facetas. El envío de múltiples SMS, los anuncios en la radio en dialectos locales, las sátiras locales y los anuncios en los periódicos son todos parte de las campañas para la concientización de los clientes. Incrementar la conciencia de los clientes a través de claras comunicaciones ha sido parte vital para el éxito de Safaricom en cuanto a manejar el fraude en contra de los clientes de M-PESA.

La comunicación interna y externa, es la segunda herramienta que el programa de dinero móvil necesita utilizar para hacer cumplir controles efectivos. Dependiendo del número y la complejidad de los controles que se han establecido, podría haber numerosas partes interesadas en el proceso. Internamente, los gerentes de dinero móvil, apoyo de la oficina administrativa, servicio al cliente y equipos de garantía de ingreso, son algunos de las partes interesadas comunes que deben estar al tanto y a los que debe estimulárseles para la comunicación de cualquier anomalía o actividad sospechosa a las partes internas relevantes.

La comunicación externa con los agentes y clientes es igualmente importante para un control preventivo efectivo. La generación de conocimiento entre los clientes acerca de cómo evitar el riesgo de fraude, constituye un control preventivo fundamental para reducir el predominio del fraude entre los clientes, tal como lo vemos en el caso de M-PESA.

Finalmente cuando se detecta un fraude o una actividad sospechosa, **debe haber procedimientos externos en funcionamiento a fin de asegurar que las actividades sospechosas reciben la prioridad adecuada.** Los procedimientos internos deben ser exhaustivos, de manera que se comparta la información y se ejecuten las acciones apropiadas. Cuando el cliente llama para quejarse porque los fondos en su cuenta han desaparecido, el centro de servicio al cliente debe saber cómo priorizar esa queja.

De igual manera, si la queja concierne a un agente específico, debe también haber un proceso establecido acerca de la disciplina de los agentes. En casos severos, si algún agente ha accedido a las cuentas del cliente mediante la sustracción de su PIN, a menudo algunos operadores de dinero móvil lo que hacen es bloquear la cuenta del agente en forma inmediata, quedando pendiente de una investigación más extensa. Para delitos menores a nivel de agentes, los operadores típicamente darán al agente un aviso antes de emprender acciones.

Cuando los controles no son una opción: transferir, tolerar o terminar con los riesgos

Si un riesgo no es aceptable, un operador puede tomar la decisión de transferir el riesgo. El seguro es una forma de transferir el riesgo, pero el más relevante para la mayoría de las operaciones de dinero móvil es la subcontratación. El uso de terceras partes (tales como agentes, compañías para el manejo de dinero u operadores para el proceso de negocios) puede reducir el riesgo para un operador. Sin embargo, muchas regulaciones pueden estipular que el banco o el operador responsable no pueden transferir algunas formas de responsabilidad.

UBL Omni: Cuándo tolerar y cuándo controlar los riesgos

En Pakistán, UBL, deseaba hallar la manera de animar a sus clientes de dinero móvil a utilizar las transacciones en los puntos de venta extrabursátiles (OTC por sus siglas en inglés) de Omni para pasar a las billeteras electrónicas. Debido a una regulación modificada, UBL pudo permitir a los nuevos clientes de Omni realizar dos transacciones antes de la verificación de la cuenta, permitiendo que ciertas transacciones fueran autenticadas por SMS. UBL decidió implementar la nueva opción como una manera de reducir las barreras para que los clientes probaran la billetera electrónica.

El equipo de fraude y riesgo reconoció que había un riesgo adicional de actividad fraudulenta al permitir que los clientes realizaran transacciones bajo ciertas circunstancias sin el uso de un PIN. El equipo decidió que el beneficio comercial excedía el riesgo y toleraron el riesgo en el lanzamiento, permitiendo algunas transacciones de bajo valor. Ellos controlaban la actividad y en el curso de la primera semana descubrieron que había unas pocas quejas por parte de algunos clientes. Estos clientes se quejaban de que las transacciones se habían completado a través de sus cuentas sin su conocimiento.

Como respuesta, el equipo de fraude y riesgo decidió implementar un control adicional. En el curso de una semana, ellos habían restringido las transacciones permitidas haciendo mandatorios los códigos de desembolso en lugar de un PIN.

UBL podía tolerar el riesgo en el lanzamiento porque sabían que ellos tenían las capacidades, debido a su tecnología, para reaccionar rápidamente si se incrementaba el impacto del riesgo percibido. Lo que es igualmente importante es que mientras UBL decidió tolerar el riesgo, ellos monitoreaban cuidadosamente la actividad para asegurarse de que estuvieran inmediatamente al tanto de cualquier impacto.

Alternativamente, hay casos en donde un servicio puede elegir tolerar un riesgo. A veces una buena opción consiste en aceptar que el riesgo ocurrirá, puesto que el análisis del costo-beneficio en cuanto a prevenir el riesgo indica que el costo o el impacto para el cliente es demasiado elevado. Si se toma esta decisión, debe ser monitoreada muy de cerca en caso de que se produzcan cambios en la ecuación de costo-beneficio.

Otra posible ruta es la terminación del riesgo cuando no es posible un control práctico y efectivo. Si un producto o servicio en particular están creando numerosas posibilidades de pérdida o fraude, cuestiones con los clientes u otros problemas, la mejor opción es a veces descontinuar ese producto. Puede ser necesario crear un esquema de precios particular o si no manejar el cambio para aquellos afectados.

Monitorear y revisar la estrategia de Gestión de Riesgo: asegurando la efectividad a largo plazo

Monitorear los controles y revisar los riesgos a lo largo del tiempo es crucial para mantener una estrategia efectiva para la mitigación del riesgo en el dinero móvil.

Preguntas a las que responder en el proceso de monitoreo

- ¿Cuáles son las nuevas actividades fraudulentas que están sucediendo? ¿Existe una tendencia?
- ¿Están todos los controles adecuadamente diseñados y ejecutados?
- ¿Están al tanto todos los empleados y gerentes y comprenden sus roles y responsabilidades?

El monitoreo requiere un sólido apoyo por parte de la gerencia y recursos internos adecuados

Primeramente, es importante que el proceso la gestión de riesgo cuente con una detallada participación de la gerencia. Numerosos operadores de dinero móvil cuentan con un dedicado Comité para la Gestión de Riesgo con integrantes de la Gerencia Superior de diferentes partes de los negocios. Esto quizás también cuente con la representación de la Junta de Directores o asociados bancarios. Debe tener una agenda permanente para revisar el actual perfil de riesgo, la efectividad de los controles y estar alerta para cualquier novedad o riesgo emergente. También puede tener un rol en la aprobación de productos o servicios nuevos o modificados. A través del proceso de gestión de riesgos, es importante que la gerencia haya validado la evaluación del riesgo y las decisiones en cuanto a la aceptación del riesgo.

Una de las formas más comunes de monitoreo, utilizada por los servicios de dinero móvil, es una auditoría interna anual. Esta es una revisión completa para asegurar que todos los procesos y controles se realizan oportunamente y son completados por un equipo que no está directamente involucrado en el servicio de dinero móvil. A menudo el equipo de auditoría interna se integra a nivel de grupo o puede ser parte del equipo de finanzas y garantía de ingresos. Los proveedores de dinero móvil pueden confiar en el mismo equipo de auditoría interna que conduce la auditoría del riesgo del lado de los negocios GSM. La última opción puede ser más atractiva para los servicios más pequeños, debido a las sinergias de los costos. Sin embargo, los operadores que utilizan este enfoque necesitan asegurarse que la auditoría GSM está apropiadamente adaptada para el dinero móvil.

Más allá de una revisión estándar de una auditoría interna, existen también formas más creativas en las que nosotros hemos visto al servicio de dinero móvil manejar el proceso de monitoreo. WING en Camboya monitorea la conciliación a través de la revisión entre pares. La manipulación de la conciliación es sin lugar a dudas uno de los mayores riesgos en dinero móvil, requiriendo una serie de controles preventivos y de investigación, incluyendo una clara separación de tareas y el control del acceso así como la actividad del sistema. En WING, los gerentes que no están directamente involucrados en el proceso, realizan la conciliación como un control al azar. Hay dos beneficios en este proceso. Primero, los gerentes se familiarizan más con los pasos necesarios para realizar la conciliación y por lo tanto tienen mayor capacidad para identificar si existen algunas irregularidades que reportar. Segundo, el gerente actúa como un controlador externo, reduciendo el riesgo de una confabulación entre aquellos que regularmente realizan la conciliación.

El monitoreo es fundamental para el éxito de la gestión de riesgos porque los programas de dinero móvil evolucionarán y, con una mayor oferta de productos o simplemente una creciente base de clientes, los controles deberán ser revisados para asegurar una continua efectividad. Igualmente importante es que mientras que el servicio cambia, también lo hace la sofisticación de los estafadores. Los operadores deben asegurar recursos adecuados para revisar, con regularidad, tanto la efectividad de los controles como el mercado para nuevas tendencias potenciales en las actividades fraudulentas. Las revisiones regulares aunadas con la activa participación de la gerencia, son ambas necesarias para que los operadores puedan asegurar una sostenibilidad a largo plazo de una efectiva gestión de riesgo.

El fraude y el riesgo son cuestiones clave que deben ser abordadas por cualquier operador de dinero móvil. Estas son las preocupaciones, no solo del operador, sino también la de los clientes, de los agentes y de los reguladores. Nuestra investigación ha demostrado que existen muchas tácticas que los operadores pueden utilizar para identificar, priorizar, controlar y monitorear el riesgo de fraudes. Al asegurarse que los fraudes son manejados de acuerdo a esta estructura, los operadores pueden protegerse a sí mismos, a sus clientes y agentes, y ayudar a contribuir al éxito de los negocios de dinero móvil.

El programa de MMU recibe apoyo de The Bill & Melinda Gates Foundation,
The MasterCard Foundation y Omidyar Network

Para mayor información, por favor ponerse en contacto con
mmu@gsma.com
GSMA London Office
T +44 (0) 20 7356 0600
http://www.gsma.com/mmu