

Artículo Destacado de la semana - 07.07.2008

Lavando a través del teléfono celular: ¿Realidad o ficción?

Por Saskia Rietbroek*

En gran parte del mundo, se puede hacer las compras de alimentos y realizar pagos de toda clase utilizando el teléfono celular. Incluso se pueden transferir fondos a otro cliente telefónico utilizando los mensajes de texto del Servicio de Mensajes Cortos (Short Message Service, o SMS). La autorización generalmente requiere marcar un número de identificación personal (PIN, por sus siglas en inglés) asociado con el cliente o el teléfono celular en cuestión. Después de realizar la operación, el cliente recibe una confirmación SMS. Parece fácil, ¿verdad?

Individual o vinculado a una cuenta bancaria

En la forma más básica del pago móvil, el cliente utiliza su teléfono como un dispositivo accesorio para iniciar y autenticar transacciones de las cuentas bancarias existentes o de las tarjetas de pago. Dado que participa una cuenta bancaria en una institución regulada, el cliente ya estaría identificado desde el momento que abrió la cuenta bancaria subyacente o la cuenta de la tarjeta de crédito. Pero la cuenta móvil también puede funcionar en forma individual sin ninguna cuenta bancaria o de pago de tarjeta relacionada con la misma. En este caso, el operador telefónico actúa como un intermediario de pago y autoriza y registra el pago en su sistema.

La modalidad individual se presenta en forma prepaga o con pago posterior. En el sistema de pago posterior, el operador telefónico autoriza al dueño del teléfono a cargar pagos en su cuenta telefónica. En el sistema prepago, el operador telefónico autoriza al dueño del teléfono a depositar fondos en una "cuenta" (ésta no es una cuenta bancaria) que tiene el operador a estos fines. En la opción individual, las compañías telefónicas que prestan el servicio posiblemente no sean supervisadas por los reguladores antilavado de dinero (ALD) de ningún país.

Metodología del lavado telefónico

El lavador de dinero puede abusar del sistema móvil de pago de esta forma: compra una tarjeta prepaga y la carga con dinero mal habido. Luego se registra en línea con un proveedor de pago móvil, utilizando una cuenta de correo electrónico anónima y gratuita, el número de teléfono móvil prepago y el dinero en una tarjeta de valor acumulado. Por supuesto, dan un número de identificación falso y un domicilio falso.

Al usar el teléfono móvil, el lavador luego se conecta en el sitio de Internet del proveedor de servicios de pago e ingresa el número de teléfono celular al cual desea transferir los fondos de la tarjeta prepagada. La compañía telefónica envía un mensaje

al número de teléfono del receptor en el cual le pregunta adónde desea enviar el dinero. Si tiene cuentas en el banco, el receptor puede solicitar que la transferencia sea hecha a su tarjeta de valor acumulado. Eso ahora le permitiría extraer los fondos en cualquier cajero automático, en cualquier lugar. La transacción no dejaría muchos rastros que pudieran ser auditados: dos números de teléfonos celulares, el monto de la transacción, unas breves instrucciones sobre la transmisión de los fondos y la recepción del dinero.

Esto crea una situación en la que existen mínimos rastros y donde hay anonimato, combinado con que funciona de manera similar a una tarjeta de débito o crédito o a un servicio de remesa. Y todo ello está virtualmente sin regular.

Medidas para mitigar el riesgo

Montos. Es más probable que exista lavado de dinero y fraude cuando los montos de las transacciones y de carga de la tarjeta son altos. Cuando los teléfonos celulares son dispositivos de acceso a cuentas bancarias o de tarjetas de crédito subyacentes, esas restricciones pueden no ser necesarias. Si los pagos móviles no están vinculados con cuentas bancarias subyacentes, el proveedor telefónico a menudo fija un monto máximo por transacción diaria - tal vez unos pocos cientos de dólares o euros - lo que limita la vulnerabilidad al lavado de dinero.

Identificación. Si el servicio de teléfono celular y los fondos utilizados para facilitar el pago móvil son prepagos, el proveedor del servicio puede no estar motivado para identificar totalmente a los clientes, porque él no tiene riesgo de crédito y no se ve obligado a cumplir obligaciones legales. Aún así, sería prudente identificar al cliente y verificar la información brindada en el proceso de inscripción. De lo contrario, el proveedor telefónico no tiene forma de saber si la información recibida es real o si fue robada a otra persona.

Método de fondeo. Los pagos móviles realizados de una cuenta prepagada pueden recibir los fondos de una cuenta bancaria o de una tarjeta de débito/crédito prepagada. Las fuentes de pago que verificaron en forma independiente la identidad del propietario del teléfono y que mantienen un registro de los fondos transferidos a la cuenta móvil presentan un riesgo bajo.

El uso de dinero en efectivo para fondear una cuenta de pago móvil, además de otros factores de riesgo, puede presentar algún peligro limitado de lavado de dinero y financiamiento del terrorismo. La restricción sobre las opciones de fondeo puede mitigar el riesgo.

Uso de límites. Generalmente, los pagos de transacciones en puntos de venta (point of sale, o POS) pueden ser aceptados solamente por los comerciantes participantes o por otros suscriptores del servicio. Los suscriptores también pueden extraer dinero a través de sus cuentas de pago móvil directamente de sus cuentas bancarias o como efectivo de los cajeros automáticos con una tarjeta prepagada. El monto máximo de la transacción y la escasa funcionalidad transfronteriza pueden ayudar a reducir el riesgo.

Detectando al lavador de teléfono celular

Las compañías telefónicas pueden no estar obligadas legalmente a hacerlo, pero sus políticas y procedimientos internos o sus acuerdos con bancos pueden obligar a reportar operaciones sospechosas. A fin de hacer esto, no sólo deben identificar al cliente, sino que también deben conservar registros de cada transacción (incluidos los micro pagos) a fin de identificar patrones de transacciones y monitorear las transacciones sospechosas.

El riesgo es la probabilidad de que una amenaza determinada ataque a una vulnerabilidad determinada y cause un daño específico. La probabilidad de que los teléfonos móviles sean usados para cometer lavado de dinero no es tan grande si se toman las medidas precautorias adecuadas. Pero si una compañía telefónica aparece en el titular de un diario vinculada a un caso de lavado de dinero o financiamiento del terrorismo, el impacto puede ser tremendo y su reputación se puede ver dañada para siempre. Sólo con una administración de riesgo adecuada las compañías pueden aislar los riesgos e identificar las posibles opciones para mitigarlo y mantenerse alejadas de los problemas.

Escenarios de detección

- Una cuenta de pago móvil puede ser utilizada para obtener dinero en efectivo a través de un cajero automático en la misma forma que una tarjeta de débito accede a una cuenta bancaria a través de un cajero automático. Eso significa que el software puede utilizar escenarios de detección similares a los utilizados para las cuentas bancarias, identificando situaciones tales como transacciones superiores a determinados montos, extracciones en el exterior combinadas con el depósito en efectivo de una suma elevada realizada en un cierto período, y las transacciones vinculadas a países de alto riesgo.
- Si una cierta cantidad límite de transacciones es realizada por un titular de cuenta determinado, una solución automática de monitoreo puede generar un alerta que hace que sea necesaria una mayor investigación. Pueden fijarse distintos límites para los titulares de cuentas de pago móvil con distintas calificaciones de riesgo.
- Puede crearse un escenario de detección fijando límites sobre la variedad aceptable de transferencias para ciertas tarjetas y generando un alerta cuando se alcanza ese límite.
- Con una red o un dispositivo de análisis vinculado, la solución automática de monitoreo puede identificar, investigar y rastrear conexiones entre los titulares de cuentas móviles. Esto puede ayudar a descubrir el rastro del lavado. También puede permitirle a la compañía establecer una revisión de las relaciones de los titulares de cuentas. ¿Quién está transmitiendo fondos a quién?
- Las soluciones automáticas de monitoreo pueden recibir y asignar calificaciones de riesgo inicial a los clientes, cuyas actividades puedan ser rastreadas. Eso le permite al personal de cumplimiento determinar si las calificaciones de riesgo inicial deben ser modificadas.

- Las soluciones automáticas de monitoreo pueden comparar la actividad del cliente en cuestión con sus perfiles históricos. También pueden comparar patrones dentro de varios grupos, como los residentes de la misma área o las personas de la misma edad u ocupación.