ESQUEMA GENERAL AMPLIADO Y PROCEDIMIENTOS DE INSPECCIÓN DE PRODUCTOS Y SERVICIOS

Cuentas Corresponsales (Nacionales): Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el ofrecimiento de relaciones de cuentas corresponsales nacionales, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Los bancos mantienen relaciones corresponsales en otros bancos nacionales para proporcionar algunos servicios que pueden realizarse de manera más económica o eficaz debido al tamaño, la pericia técnica en un rubro de la actividad comercial específico o la ubicación geográfica del otro banco. Dichos servicios pueden incluir:

- **Cuentas de depósito.** Los activos conocidos como "efectivo en depósitos bancarios" o "saldos en bancos corresponsales" pueden representar la cuenta principal de operaciones del banco.
- **Transferencias de fondos.** Una transferencia de fondos entre bancos puede ser el resultado del cobro de cheques u otros instrumentos en efectivo, transferencia y liquidación de transacciones de valores, transferencia de fondos de préstamos participables, compra o venta de fondos federales o procesamiento de transacciones de los clientes.
- **Otros servicios.** Los servicios incluyen el procesamiento de participaciones de préstamos, la facilitación de ventas de préstamos de mercado secundarios, el procesamiento de datos y servicios de nómina y el cambio de moneda extranjera.

Bancos de los banqueros

Un banco de los banqueros, que está organizado y constituido para negociar con otros bancos, por lo general es propiedad de los bancos a los que le ofrece servicios. Los bancos de banqueros, que no negocian directamente con el público, ofrecen servicios bancarios corresponsales a bancos comunitarios independientes, instituciones de ahorro y crédito, cooperativas de crédito y préstamo y fideicomisos de inversión de bienes inmuebles. Los bancos de los banqueros prestan servicios directamente, mediante contratación tercerizada o a través del patrocinio o aval otorgado a terceros. Los productos que ofrecen los bancos de los banqueros por lo general consisten en servicios tradicionales de bancos corresponsales. Los bancos de los banqueros deben tener políticas, procedimientos y procesos en función del riesgo para gestionar los riesgos BSA/AML planteados en estas relaciones corresponsales, detectar e informar actividades sospechosas.

Por lo general, un banco de los banqueros firma un acuerdo de servicio con el banco respondiente[160] describiendo las responsabilidades de cada parte. El acuerdo de servicios puede incluir lo siguiente:

- Productos y servicios que se ofrecen.
- Responsabilidad de la gestión de registros (por ejemplo, informes de transacciones en efectivo presentados).
- Responsabilidad de las tareas realizadas (por ejemplo, filtrados según la OFAC).
- Control de la documentación supervisada (por ejemplo, informes de consultores y de auditoría).

Factores de riesgo

Debido a que los bancos nacionales deben seguir las mismas exigencias normativas, los riesgos BSA/AML en los bancos corresponsales nacionales, incluidos los bancos de los banqueros, son mínimos en comparación a otros tipos de servicios financieros, especialmente para las cuentas de propiedad privada (es decir, el banco nacional utiliza la cuenta corresponsal para sus propias transacciones). Cada banco, sin embargo, tiene su propio enfoque para realizar su programa de cumplimiento BSA/AML, que incluye debida diligencia de los clientes, los sistemas para la información de gestión, la supervisión de cuentas y los informes de actividades sospechosas. Además, si bien es posible que las cuentas corresponsales nacionales no se consideren de riesgo más alto, las transacciones realizadas a través de esas cuentas, que pueden ser realizadas en nombre del cliente de banco representado, pueden implicar riesgo más alto. Los riesgos de lavado de dinero pueden aumentar cuando un banco respondiente le permite a sus clientes efectuar o ejecutar transacciones mediante la cuenta corresponsal, especialmente cuando dichas transacciones son efectuadas o ejecutadas mediante una cuenta de propiedad privada aparente.

El banco corresponsal también enfrenta un aumento en los riesgos cuando proporciona envíos de moneda directos a clientes de bancos respondientes. Esto no significa que esas actividades impliquen necesariamente lavado de dinero, sino que esos envíos de moneda directos deben ser supervisados de manera apropiada en busca de actividades sospechosas y poco habituales. Sin dicho sistema de supervisión, el banco corresponsal está esencialmente proporcionando estos servicios directos a un cliente desconocido.

Mitigación del riesgo

Los bancos que ofrecen servicios bancarios corresponsales a otros bancos respondientes deben disponer de políticas, procedimientos y procesos para gestionar los riesgos BSA/AML que surgen en estas relaciones corresponsales y para detectar e informar actividades sospechosas. Los bancos deben cerciorarse de que las cuentas corresponsales

[160] A respondent bank is any bank for which another bank establishes, maintains, administers, or manages a correspondent account relationship.

nacionales sean de propiedad privada o permitan transacciones de terceros. Cuando el banco respondiente permite a clientes de terceros hacer negocios a través de cuentas corresponsales, el banco corresponsal debe garantizar que comprende los procedimientos de supervisión y debida diligencia aplicados por el banco respondiente a sus clientes que utilizarán la cuenta.

El nivel de riesgo varía dependiendo de los servicios proporcionados y los tipos de transacciones realizadas a través de la cuenta; así como del programa de cumplimiento BSA/AML, productos, servicios, clientes, entidades y ubicaciones geográficas del banco respondiente. Cada banco debe supervisar de manera adecuada las transacciones de cuentas corresponsales nacionales con relación al nivel del riesgo analizado. Además, los bancos nacionales son responsables de manera independiente del cumplimiento de la OFAC de cualquier transacción que fluya a través de sus bancos. Se debe disponer de un filtrado adecuado. Consulte la sección del esquema general principal y los procedimientos de inspección, “Oficina de control de activos extranjeros”, en las páginas 165 a 175 y 176 a 178, respectivamente.

Procedimientos de Inspección

Cuentas corresponsales (nacionales)

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el ofrecimiento de relaciones de cuentas corresponsales nacionales, y de la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos y cualquier acuerdo de servicio bancario relativo a las relaciones de bancos corresponsales nacionales. Evalúe la aptitud de las políticas, procedimientos y procesos en relación con las cuentas corresponsales nacionales del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y de los factores de valoración de riesgos internos, determine si el banco ha identificado alguna actividad de los bancos corresponsales nacionales como de riesgo más alto.

3. Determine si el sistema del banco para supervisar las cuentas corresponsales nacionales en busca de actividades sospechosas, y para informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del control del banco de las cuentas de bancos respondientes[161] para detectar actividad poco habitual o de riesgo más alto, su análisis de riesgos y los informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de bancos respondientes. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise los estados de cuenta del banco de las cuentas corresponsales nacionales.
   - Revise las transacciones de grandes volúmenes o poco habituales para determinar su carácter. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.

[161] Un banco respondiente es todo banco para el cual otro banco establece, mantiene, administra o gestiona una relación de cuenta corresponsal.

- Tenga en cuenta cualquier envío de moneda o depósitos realizados en nombre del cliente del banco respondiente. En función de esta información determine si:
  - Los envíos de moneda están documentados de manera adecuada.
  - El banco respondiente ha implementado debida diligencia en los clientes que realizan importantes transacciones en efectivo.
  - Los informes de transacciones en efectivo están presentados de manera adecuada y la actividad es acorde a la actividad prevista.

6. Revise los estados de cuenta del banco para los registros de cuentas corresponsales nacionales o registros de télex de cuentas controladas por la misma persona para depósitos importantes de cheques de caja, giros postales o instrumentos similares librados por otros bancos en sumas inferiores a USD 10.000. Estos fondos serán transferidos probablemente a otra parte en grandes cantidades. Tenga en cuenta si los instrumentos por debajo de USD 10.000 están numerados secuencialmente.
7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de los bancos corresponsales nacionales.

Cuentas Corresponsales (Extranjeras): Esquema General

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los bancos corresponsales extranjeros, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe. Esta sección amplía la revisión principal anterior de las exigencias normativas y legales de las relaciones asociadas con cuentas de bancos corresponsales para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

Las instituciones financieras extranjeras mantienen cuentas en los bancos estadounidenses para acceder al sistema financiero de ese país y aprovechar servicios y productos que pueden no estar disponibles en la jurisdicción de la institución financiera extranjera. Estos servicios pueden ser realizados de manera más económica o eficiente por el banco estadounidense o pueden ser necesarios por otros motivos, como para facilitar el comercio internacional. Los servicios pueden incluir:

- Servicios de administración de efectivo, que incluyen cuentas de depósito.
- Transferencias internacionales de fondos.
- Compensación *(Clearing)* de cheques.
- Cuentas empleadas para pagos.
- Depósitos vía maletines/bolsos.
- Servicios de cambio de moneda extranjera.
- Cuentas de inversión automática (cuentas con servicio de barrido).
- Préstamos y cartas de crédito.

Acuerdos contractuales

Cada relación que un banco estadounidense mantenga con instituciones financieras corresponsales extranjeras debe regirse por un acuerdo o contrato que especifique las obligaciones de cada una de las partes y otros detalles de la relación (por ejemplo, productos y servicios que se ofrecerán, aceptación de depósitos, compensación de elementos, formas de pago y tipos de endoso que se aceptarán). El acuerdo o contrato debe también considerar las exigencias normativas AML de la institución financiera extranjera, el tipo de clientela, los procedimientos de debida diligencia y el uso autorizado de la cuenta corresponsal por terceros.

Factores de riesgo

Algunas instituciones financieras extranjeras no están sujetas a las mismas pautas normativas que se aplican a los bancos estadounidenses; por lo tanto, esas instituciones pueden representar un riesgo de lavado de dinero mayor para su respectivo banco corresponsal estadounidense o sus respectivos bancos estadounidenses. Se han realizado investigaciones que demuestran que, en el pasado, las cuentas corresponsales extranjeras han sido utilizadas por narcotraficantes y otros delincuentes para lavar fondos. A veces se usan compañías fantasmas en el proceso de transformación para ocultar la verdadera propiedad de las cuentas en las instituciones financieras corresponsales extranjeras. Debido al gran volumen de fondos, las múltiples transacciones y la posible falta de familiaridad de los bancos estadounidenses con los clientes de las instituciones financieras corresponsales extranjeras, los delincuentes y terroristas pueden ocultar con mayor facilidad el origen y la utilización de los fondos ilícitos. Por lo tanto, cada banco estadounidense, incluso todas las sucursales, oficinas y subsidiarias en el exterior, debe supervisar cuidadosamente las transacciones relacionadas con las cuentas corresponsales extranjeras.

Sin los controles adecuados, puede ocurrir que los bancos estadounidenses abran cuentas corresponsales tradicionales en una institución financiera extranjera sin saber que ésta les permite a algunos clientes realizar transacciones en forma anónima a través de la cuenta del banco estadounidense (por ejemplo, cuentas para realizar pagos[162] y cuentas anidadas).

Cuentas anidadas

Las cuentas anidadas se producen cuando una institución financiera extranjera logra acceder al sistema financiero de los Estados Unidos operando a través de una cuenta corresponsal estadounidense que pertenece a otra institución financiera extranjera. Si el banco estadounidense desconoce que la institución financiera corresponsal extranjera que es cliente suyo permite dicho acceso a instituciones financieras extranjeras ajenas a esa relación (terceros), éstas pueden efectivamente acceder en forma anónima al sistema financiero estadounidense. El comportamiento que indica la existencia de cuentas anidadas y otras cuentas que despiertan alarma incluye transacciones dirigidas a jurisdicciones en las cuales la institución financiera extranjera no tiene actividades comerciales conocidas ni intereses, y transacciones cuyo volumen total y frecuencia supera significativamente la actividad prevista de la institución financiera extranjera, teniendo en cuenta su base de clientes y el tamaño de sus activos.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen los servicios de instituciones financieras extranjeras corresponsales deben disponer de políticas, procedimientos y procesos para gestionar los riesgos BSA/AML inherentes a estas relaciones, y deben supervisar cuidadosamente las transacciones relacionadas con estas cuentas para detectar e informar

[162] Consulte la sección del esquema general ampliado, “Cuentas empleadas para pagos”, en las páginas 221 a 223, como guía.

actividades sospechosas. El nivel de riesgo varía según los productos, servicios, clientes y ubicación geográfica de la institución financiera extranjera. The Clearing House Payments Co., LLC. y el Grupo Wolfsberg han publicado las normas de la industria y las pautas sugeridas para bancos que prestan servicios bancarios corresponsales extranjeros.[163] Además, la sección del esquema general principal "Debida diligencia y gestión de registros de cuentas corresponsales extranjeras" de las páginas 130 a 138 contiene información adicional. Las políticas, los procedimientos y los procesos de los bancos estadounidenses deben:

- Especificar los procedimientos adecuados de apertura de cuentas, que pueden incluir niveles mínimos de documentación a obtenerse de los clientes probables, un proceso de aprobación de cuenta independiente del rubro de la actividad comercial de la cuenta corresponsal para posibles clientes de riesgo más alto, y una descripción de las circunstancias en las que el banco no abrirá una cuenta.

- Evaluar los riesgos que plantean las relaciones de clientes de cuentas corresponsales extranjeras probables empleando metodologías de análisis de riesgos bien documentadas y coherentes, e incorporar esa determinación del riesgo en el sistema de supervisón de actividades sospechosas del banco.

- Comprender el uso deseado de las cuentas y la actividad de la cuenta prevista (por ejemplo, determinar si la relación ofrecerá servicios de cuenta empleada para pagos).

- Comprender las otras relaciones corresponsales de la institución financiera corresponsal extranjera (por ejemplo, determinar si se podrán utilizar cuentas anidadas).

- Realizar debida diligencia adecuada y continua en las relaciones de la institución financiera corresponsal extranjera, que puede incluir visitas periódicas.

- Establecer un proceso formal para derivar información sospechosa sobre clientes existentes y potenciales a un nivel de gestión apropiado para su control.

- Garantizar que las relaciones de instituciones financieras corresponsales extranjeras estén incluidas de manera apropiada dentro de los sistemas de informe y supervisión de actividades sospechosas del banco estadounidense.

- Garantizar que se apliquen las normas de debida diligencia apropiadas a aquellas cuentas determinadas como de riesgo más alto.

- Establecer criterios para cerrar cuentas de instituciones financieras corresponsales extranjeras.

---

[163] Consulte *Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking* (Pautas para las políticas y procedimientos contra el lavado de dinero en los bancos corresponsales), de Marzo de 2002, en www.theclearinghouse.org/docs/000592.pdf y *Wolfsberg AML Principles for Correspondent Banking* (Principios AML de Wolfsberg para los bancos corresponsales), de Noviembre de 2002, en www.wolfsberg-principles.com/standards.html.

Como práctica responsable, se exhorta a los bancos estadounidenses a comunicar sus expectativas relacionadas con AML a sus clientes de instituciones financieras corresponsales extranjeras. Por otra parte, el banco estadounidense debe comprender en general los controles AML en la institución financiera corresponsal extranjera, que incluyen prácticas de debida diligencia de los clientes y gestión de registros documentales.

Procedimientos de Inspección

Cuentas corresponsales (extranjeras)

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los bancos corresponsales extranjeros, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe. Esta sección amplía la revisión principal anterior de las exigencias normativas y legales de las relaciones asociadas con cuentas de bancos corresponsales para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras. Evalúe la aptitud de las políticas, los procedimientos y los procesos. Analice si los controles son adecuados para proteger razonablemente al banco estadounidense del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco estadounidense identifica y supervisa de manera eficaz las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras, particularmente aquellas que planteen un riesgo más alto de lavado de dinero.

3. Si el banco estadounidense tiene un acuerdo con bancos corresponsales extranjeros estándar, revise un acuerdo de muestra para determinar si las responsabilidades, los productos y los servicios prestados por cada parte, y el uso permitido de terceros de la cuenta corresponsal, están cubiertos por el acuerdo contractual. Si el banco estadounidense no tiene un acuerdo estándar, consulte los procedimientos de inspección de las pruebas de transacciones.

4. Determine si el sistema del banco estadounidense para supervisar las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras, detectar e informar de actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus actividades con bancos corresponsales extranjeros, así como de informes de inspecciones previas y de auditoría, seleccione una muestra de las relaciones asociadas con cuentas de instituciones financieras corresponsales extranjeras de riesgo más alto. La muestra de riesgo más alto debe incluir las relaciones con instituciones financieras extranjeras ubicadas en jurisdicciones que no cooperan con las iniciativas AML internacionales y en otras jurisdicciones que el banco estadounidense haya considerado que presentan

un riesgo mayor. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise un acuerdo con bancos corresponsales extranjeros o un contrato que delimite las responsabilidades y los productos y servicios proporcionados por cada parte.
- Revise los estados de cuenta del banco estadounidense para verificar las cuentas corresponsales extranjeras y, según sea necesario, detalles específicos de las transacciones. Compare las transacciones previstas con la actividad real.
- Determine si la actividad real es coherente con el tipo de negocio del cliente. Identifique cualquier actividad sospechosa o poco habitual.
- Revise las transacciones de grandes volúmenes o poco habituales para determinar su carácter. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.
- Analice transacciones para identificar un comportamiento que indique la existencia de cuentas anidadas, servicios de agente de compensación o intermediario, u otros servicios para instituciones financieras extranjeras externas que no se hayan identificado claramente.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con relaciones con instituciones financieras corresponsales extranjeras.

Envíos de Efectivo en Grandes Cantidades: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con la recepción de envíos de efectivo en grandes cantidades y la implementación por parte de la gerencia de sistemas eficaces de supervisión e informe.*

Los envíos de efectivo en grandes cantidades implican la utilización de empresas de transporte aéreo, terrestre o marítimo, comunes, independientes o pertenecientes al Servicio Postal, para transportar grandes volúmenes de papel moneda (estadounidense o extranjero) desde fuentes ubicadas dentro o fuera de los Estados Unidos a un banco en los Estados Unidos. A menudo, pero no siempre, los envíos se realizan en contenedores.

Los expedidores pueden ser "remitentes de moneda", es decir, personas o empresas que generan efectivo a partir de la venta al contado de materias primas, u otros productos o servicios (incluidos los instrumentos monetarios o los cambios de moneda). También pueden ser "intermediarios" que envían el efectivo que recolectan de sus clientes remitentes de moneda. Además, los intermediarios pueden enviar el efectivo que recolectan de otros intermediarios. Los intermediarios pueden ser otros bancos, los bancos centrales, las instituciones financieras que no están destinadas al depósito o agentes de estas entidades.

Los bancos reciben los envíos de efectivo en grandes cantidades de manera directa cuando toman posesión de un envío real, y los reciben de manera indirecta cuando toman posesión del equivalente económico de un envío de efectivo, por ejemplo, mediante una notificación de carta de remesa. En el caso de un envío recibido de manera indirecta, generalmente el envío real se traslada al Banco de la Reserva Federal o una sucursal, donde se registra como acreditado a nombre del banco.

Los bancos tienen la obligación de declarar los envíos de efectivo por un importe acumulado superior a USD 10.000 recibidos desde o enviados a ubicaciones que están fuera de los Estados Unidos mediante el Formulario 105 de la FinCEN (Informe sobre el transporte internacional de moneda o instrumentos monetarios), y están exentos de cumplir con esta exigencia de declaración cuando el efectivo se envía por vía terrestre mediante una empresa de transporte común o el Servicio Postal (consulte 31 CFR 103.23). Los bancos no están exentos de cumplir con esta exigencia de declaración cuando el efectivo se envía mediante otros métodos, como las aerolíneas o una empresa de transporte aéreo. Independientemente de que se aplique o no la exención de presentar el Formulario 105 de la FinCEN, los bancos deben supervisar e informar cualquier actividad sospechosa. Además, sin considerar la exigencia de declaración mediante este formulario, los bancos deben informar toda recepción o desembolso de moneda superior a USD 10.000 mediante el Formulario 104 de la FinCEN (Informe de transacciones en efectivo), sujeto a las exenciones de 31 CFR 103.122(d). Esta exigencia de declaración se aplica incluso si las transacciones internacionales están sujetas a la exención de presentar el Formulario 105.

Factores de riesgo

Los envíos de efectivo en grandes cantidades a los bancos por parte de expedidores que se suponen honrados pueden, de todas maneras, originarse a partir de una actividad ilícita. Por ejemplo, frecuentemente los ingresos monetarios resultantes de actividades delictivas reaparecen en el sistema financiero como fondos aparentemente legítimos que han sido colocados y finalmente integrados mediante su circulación a través de numerosos intermediarios y transacciones transformadas que ocultan el origen de los fondos. Las fases de transformación pueden incluir envíos desde y hacia otras jurisdicciones. Consecuentemente, los bancos que reciben envíos de efectivo en grandes cantidades de manera directa o indirecta corren el riesgo de ser coautores en las estratagemas de lavado de dinero y financiamiento del terrorismo.

En los últimos años, el contrabando de efectivo en grandes cantidades se ha convertido en el método preferido para trasladar fondos ilícitos a través de las fronteras.[164] Debido a que las grandes cantidades de efectivo que se contrabandean fuera de los Estados Unidos generalmente son en dólares estadounidenses, quienes reciben dichas cantidades deben encontrar la forma de reintegrar la moneda en un banco estadounidense. A menudo, esto ocurre mediante el uso de una institución financiera extranjera que deliberada o involuntariamente recibe los ingresos ilícitos en dólares estadounidenses y luego emite un instrumento de carta de remesa (o realiza una transferencia de fondos) para su procesamiento (o depósito) en un banco estadounidense. Posteriormente, la institución financiera extranjera inicia el proceso de repatriar físicamente (enviar) el efectivo de regreso a los Estados Unidos.[165] La experiencia a demostrado una correlación directa entre el contrabando de efectivo en grandes cantidades, el aumento del uso de los instrumentos de carta de remesa o las transferencias electrónicas de ciertas instituciones financieras extranjeras, y los envíos de grandes cantidades de efectivo a los Estados Unidos por parte de las mismas instituciones.[166]

---

[164] El lavado de dinero y la evaluación de amenazas en los Estados Unidos, Diciembre de 2005, página 33. El Congreso penalizó el contrabando de grandes cantidades de efectivo como parte de la Ley PATRIOTA de EE. UU. Específicamente, la sección 5332 del Título 31 del U.S.C. sobre el contrabando de efectivo en grandes cantidades establece que es un delito contrabandear o intentar contrabandear un importe superior a USD 10.000 en moneda u otros instrumentos monetarios hacia o desde los Estados Unidos, con el propósito específico de evadir las exigencias de declaración de moneda estadounidense estipuladas en 31 U.S.C. 5316.

[165] En algunos casos, la institución financiera extranjera enviará el efectivo a su banco central o un banco ubicado en uno de los centros financieros del país extranjero en el que se originó el instrumento de carta de remesa. En ocasiones, se realizan varias transacciones trasformadas para ocultar el origen del efectivo, después de las cuales la moneda puede devolverse directamente a los Estados Unidos o puede ser enviada hacia o a través de otras jurisdicciones. El efectivo será enviado a los Estados Unidos a nombre del banco estadounidense donde se procesó el instrumento de carta de remesa o donde se realizó el depósito de la transferencia de fondos.

[166] Si desea ver un ejemplo de estos tipos de transacciones, consulte la Evaluación nacional de amenaza de las drogas 2008 acerca del financiamiento ilícito del Centro Nacional de Inteligencia sobre Droga, Diciembre de 2007.

El envío de efectivo en grandes cantidades no es necesariamente indicativo de una actividad delictiva o terrorista. Muchas personas y empresas, nacionales y extranjeras, generan efectivo a partir de ventas legítimas al contado de materias primas, u otros productos o servicios. Además, los intermediarios recolectan y envían el efectivo de uno o más remitentes de moneda cuyas actividades son legítimas. Los bancos pueden ofrecer servicios en forma legítima para recibir tales envíos. Sin embargo, los bancos deben tener presente el posible uso indebido de sus servicios por parte de los expedidores de efectivo en grandes cantidades. Además, deben protegerse contra la incorporación de los ingresos monetarios resultantes de actividades delictivas o terroristas en el sistema financiero. Con el objeto de informar a los bancos sobre el tema de los envíos de efectivo en grandes cantidades, en 2006 la FinCEN emitió un comunicado que incluye algunas actividades que pueden estar asociadas con el contrabando de efectivo.[167] Según la FinCEN, las autoridades de aplicación de las leyes estadounidenses han observado un aumento significativo en el contrabando de grandes cantidades de efectivo producto de la venta de narcóticos y otras actividades delictivas desde los Estados Unidos hacia México. Si bien el comunicado de la FinCEN menciona específicamente el envío de efectivo en grandes cantidades desde y hacia los Estados Unidos y México, los temas tratados pueden aplicarse también al envío de grandes cantidades de efectivo desde y hacia otras jurisdicciones.

Las autoridades de aplicación de la ley han identificado las siguientes actividades que, en diversas combinaciones, pueden estar asociadas con el contrabando de efectivo:[168]

- Un incremento en la venta de papel moneda estadounidense de alta denominación a instituciones financieras extranjeras por parte de bancos estadounidenses.

- El canje de papel moneda estadounidense de baja denominación que ha sido contrabandeado a un país extranjero por papel moneda estadounidense de alta denominación en posesión de instituciones financieras extranjeras.

- El envío de grandes volúmenes de papel moneda estadounidense de baja denominación desde instituciones financieras no bancarias a sus cuentas estadounidenses vía transporte blindado o su venta directa a bancos estadounidenses.

- Transferencias electrónicas múltiples iniciadas por instituciones financieras extranjeras no bancarias que dan instrucciones a bancos estadounidenses para que remitan fondos a otras jurisdicciones que no parecen tener ninguna relación comercial aparente con esa institución financiera no bancaria extranjera (los receptores de transferencias de fondos incluyen individuos, empresas y otras entidades en áreas de libre comercio y otras ubicaciones).

- El canje de papel moneda estadounidense de baja denominación por papel moneda estadounidense de alta denominación que podría enviarse a países extranjeros.

---

[167] *Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States* (Guía para las instituciones financieras sobre la repatriación de moneda introducida de contrabando a México desde los Estados Unidos) de la FinCEN, FIN-2006-A003, 28 de Abril de 2006.

[168] *Id.*

- Depósitos efectuados por instituciones financieras extranjeras no bancarias en sus cuentas en bancos estadounidenses que incluyen elementos de terceros (entre ellos, instrumentos monetarios numerados en secuencia).

- Depósitos de moneda y elementos de terceros por parte de instituciones financieras extranjeras no bancarias en sus cuentas en instituciones financieras extranjeras y posteriores transferencias bancarias electrónicas directas a las cuentas de la institución financiera extranjera no bancaria en bancos estadounidenses.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen servicios para recibir envíos de efectivo en grandes cantidades deben tener políticas, procedimientos y procesos que permitan mitigar y gestionar los riesgos BSA/AML asociados con la recepción de envíos de efectivo en grandes cantidades. Además, los bancos deben supervisar de cerca las transacciones de envío de efectivo en grandes cantidades con el objeto de detectar e informar cualquier actividad sospechosa, poniendo especial atención en el origen de los fondos y en la adecuación de los volúmenes de transacción por parte de los remitentes de moneda y los intermediarios.

La mitigación del riesgo comienza con un proceso de análisis de riesgos eficaz que permita distinguir las relaciones y las transacciones que presenten un mayor riesgo de lavado de dinero o financiamiento del terrorismo. Los procesos de análisis de riesgos deben considerar la propiedad de los remitentes de moneda y los intermediarios, las geografías, y la naturaleza, el origen, la ubicación y el control de las grandes cantidades de efectivo. Para obtener información adicional relacionada con el análisis de riesgos y la debida diligencia, consulte las secciones del esquema general principal “Análisis de riesgos BSA/AML” en las páginas 23 a 33, y “Debida diligencia de los clientes” en las páginas 69 a 71.

Las políticas, los procedimientos y los procesos de un banco estadounidense deben:

- Especificar los procedimientos adecuados de establecimiento de relaciones en función del riesgo, que pueden incluir niveles mínimos de documentación que deberán proporcionar los posibles remitentes de moneda e intermediarios; un proceso de aprobación de las relaciones que, en el caso de las relaciones con un posible riesgo más alto, sea independiente del rubro de la actividad comercial y pueda incluir una visita al probable expedidor o a los sitios de preparación de los envíos; y una descripción de las circunstancias en las que el banco no establecerá una relación.

- Determinar el fin deseado de la relación , los volúmenes previstos, la frecuencia de la actividad derivada de las transacciones, los orígenes de los fondos, la adecuación de los volúmenes en función de los remitentes y los expedidores, y las obligaciones de presentación de informes según la BSA (CTR, CMIR, etc.).

- Identificar las características de las transacciones aceptables y no aceptables, incluidas las circunstancias en las que el banco aceptará o no los envíos de efectivo en grandes cantidades.

- Evaluar los riesgos que plantea una probable relación de envío mediante metodologías de análisis de riesgos bien documentadas y coherentes.
- Incorporar los análisis de riesgos, según corresponda, en la debida diligencia de los clientes del banco, la EDD y los sistemas de supervisión de actividades sospechosas.
- Una vez establecida la relación, exigir una debida diligencia adecuada y continua que, según corresponda, puede incluir visitas periódicas al expedidor y a los sitios de preparación de los envíos. Según sea necesario, realizar el escrutinio de la legitimidad del origen de los envíos de efectivo mediante procesos basados en el riesgo.
- Garantizar que se apliquen las normas de debida diligencia apropiadas a las relaciones determinadas como de riesgo más alto.
- Incluir los procedimientos para el procesamiento de los envíos, que incluyen las responsabilidades de los empleados, los controles, las exigencias de conciliación y documentación, y las autorizaciones de la gerencia para los empleados.
- Establecer un proceso formal para derivar la información sospechosa sobre las relaciones y las transacciones que involucran a remitentes de moneda e intermediarios existentes y potenciales a un nivel de gestión apropiado para su control.
- Rechazar los envíos cuyos orígenes son sospechosos o cuestionables.
- Asegurar la inclusión de las relaciones de envío y las comparaciones de los volúmenes de envío previstos y reales, según corresponda, en los sistemas de los bancos estadounidenses con el objeto de supervisar e informar las actividades sospechosas.
- Establecer los criterios para finalizar una relación de envío.

Como práctica responsable, los bancos estadounidenses deben informar a los remitentes de moneda y a los intermediarios acerca de las expectativas y las exigencias relacionadas con BSA/AML que se aplican a los bancos estadounidenses. Los bancos estadounidenses también deben comprender los controles de BSA/AML que se aplican a, o que de lo contrario son adoptados por, el remitente de moneda o el intermediario, que incluyen la debida diligencia de los clientes, y las prácticas o las obligaciones relacionadas con la gestión de registros.

También puede haber otros controles que sean útiles para proteger a los bancos contra los envíos ilícitos de grandes cantidades de efectivo, entre los que se pueden incluir los controles de los bancos corresponsales extranjeros, los depósitos vía maletines/bolsos, las transferencias de fondos, las transacciones internacionales de compensación automatizada y la captura de depósitos remotos.

Acuerdos contractuales

Los bancos estadounidenses deben establecer acuerdos o contratos con los remitentes de moneda o los intermediarios. El acuerdo o contrato debe describir las responsabilidades de cada parte y demás detalles relevantes de la relación. Además, debe reflejar y ser coherente con las consideraciones de BSA/AML que se aplican al banco, el remitente de moneda o el intermediario, y los clientes del intermediario o el remitente de moneda. Asimismo, debe cubrir las expectativas acerca de la debida diligencia y el permiso de uso de los servicios del expedidor por parte de terceros. Si bien los acuerdos y los contratos también deben proporcionar las consideraciones, obligaciones y controles de BSA/AML respectivos, los bancos estadounidenses no pueden ceder sus responsabilidades según BSA/AML a otros.

Procedimientos de Inspección

Envíos de efectivo en grandes cantidades

Objetivo: *Evaluar la aptitud de los sistemas de los bancos estadounidenses para gestionar los riesgos asociados con los envíos de efectivo en grandes cantidades, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, debida diligencia e informe.*

1. Determine si el banco recibe envíos de efectivo en grandes cantidades.

2. Revise la aptitud de las políticas, los procedimientos y los procesos relacionados con la recepción de envíos de efectivo en grandes cantidades, dados la actividad y los riesgos presentes.

3. Revise la lista de remitentes de moneda e intermediarios que envían efectivo en grandes cantidades al banco.

4. Determine si la gerencia ha analizado los riesgos asociados con la recepción de envíos de efectivo en grandes cantidades de remitentes de moneda e intermediarios. Tenga en cuenta el origen del dinero del remitente de moneda o el intermediario y la adecuación de los volúmenes de transacción. Evalúe la aptitud de la metodología de análisis de riesgos.

5. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones con los remitentes de moneda y los intermediarios, particularmente aquellas que presenten un riesgo más alto de lavado de dinero o financiamiento del terrorismo.

6. Si el banco tiene un acuerdo o un contrato con remitentes de moneda o intermediarios, revise un acuerdo o un contrato de muestra para determinar si las responsabilidades, los productos y los servicios provistos de cada parte, y el uso permitido de terceros de la relación, incluidas las responsabilidades de BSA/AML de las partes, están cubiertos. Si el banco estadounidense no tiene un acuerdo o un contrato estándar, consulte los procedimientos de inspección de las pruebas de transacciones a continuación.

7. Determine si el sistema del banco para supervisar e informar las actividades sospechosas relacionadas con las relaciones y las transacciones de envío es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

8. Determine si el banco está supervisando los volúmenes de envío reales en comparación con los previstos y si está tomando medidas ante los aumentos excesivos o poco habituales en los volúmenes.

Pruebas de transacciones

9. En función del análisis de riesgos del banco de sus relaciones con los remitentes de moneda y los intermediarios, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los remitentes de moneda o los intermediarios, y de los últimos envíos de efectivo en grandes cantidades. La muestra debe incluir relaciones con remitentes de moneda e intermediarios que estén ubicados en jurisdicciones que puedan plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo o que realicen envíos desde dichas jurisdicciones, o que participen en actividades comerciales que puedan plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo.

10. Preferentemente sin previo aviso y durante un período de varios días, no necesariamente consecutivos, observe el proceso de aceptación de envíos de efectivo en grandes cantidades. Revise los registros y los envíos en busca de irregularidades. A partir de las muestras seleccionadas, lleve a cabo los siguientes procedimientos de inspección:

    - Revise la integridad de un acuerdo o un contrato de relación que delimite las responsabilidades, los productos y los servicios provistos de cada parte.

    - Revise los estados de cuenta del banco estadounidense y, según sea necesario, los detalles específicos de las transacciones.

    - Revise los registros de control de la bóveda con relación a las transacciones de envío de efectivo en grandes cantidades (depósitos y extracciones) para identificar la actividad de alta denominación como resultado de los cambios de billetes de baja denominación.

    - Evalúe la adecuación de la información de debida diligencia de los clientes y EDD concerniente a los remitentes de moneda y los intermediarios de la muestra.

    - Determine si la naturaleza, el volumen y la frecuencia de la actividad con coherentes con las expectativas asociadas al remitente de moneda y al intermediario. Hable con la gerencia del banco sobre cualquier incoherencia identificada. Según sea necesario, obtenga y revise las copias de notas de crédito o débito, los tiquetes de libro mayor y otra documentación respaldatoria.

    - Revise las transacciones poco habituales y la información de debida diligencia de los clientes para determinar si las transacciones son potencialmente sospechosas.

    - Hable con la gerencia sobre las conclusiones y los resultados preliminares.

11. Si el remitente de moneda o el intermediario, o el agente referente que trabaja para el remitente de moneda o el intermediario, tienen una cuenta en el banco, revise una muestra de la actividad de la cuenta.

12. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con el envío de efectivo en grandes cantidades.

Giros en Dólares Estadounidenses: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los giros en dólares estadounidenses, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Un giro en dólares estadounidenses es un giro o cheque bancario en dólares estadounidenses disponible en instituciones financieras extranjeras. Estos giros se libran de una cuenta corresponsal estadounidense por una institución financiera extranjera. Los giros se adquieren con frecuencia para pagar transacciones personales o comerciales, y para conciliar obligaciones en el exterior.

Factores de riesgo

La mayoría de los giros en dólares estadounidenses son legítimos; sin embargo, se ha comprobado que éstos son vulnerables al abuso del lavado de dinero. Dichas estratagemas relacionadas con los giros en dólares estadounidenses pueden involucrar el contrabando de moneda estadounidense a instituciones financieras extranjeras para la compra de un cheque o giro en dólares estadounidenses. La institución financiera extranjera acepta la moneda estadounidense y expide un giro en dólares estadounidenses librado de su cuenta de banco corresponsal estadounidense. Una vez que el dinero se encuentra en la forma de giro bancario, la persona implicada en el lavado de dinero puede ocultar más fácilmente el origen de los fondos. La capacidad de convertir ingresos ilícitos a un giro bancario en una institución financiera extranjera permite que el lavador de dinero transporte el instrumento nuevamente a los Estados Unidos o lo endose a un tercero en una jurisdicción donde las leyes contra el lavado de dinero o de cumplimiento son laxas. En cualquier caso, el individuo habrá blanqueado los ingresos ilícitos; finalmente, el giro o cheque se devolverá para su procesamiento en el banco corresponsal estadounidense.

Mitigación del riesgo

Las políticas, los procedimientos y los procesos de un banco estadounidense deben incluir lo siguiente:

- Descripción de los criterios para iniciar una relación asociada con giros en dólares estadounidenses con una institución o entidad financiera extranjera (por ejemplo: jurisdicción; productos, servicios, mercado objetivo; propósito de la cuenta y actividad prevista; o antecedentes del cliente).
- Especificación de las transacciones aceptables y no aceptables (por ejemplo, el fraccionamiento de las transacciones o la compra de múltiples giros numerados en secuencia para el mismo beneficiario).
- Especificación de la supervisión y elaboración de informes de actividades sospechosas asociadas con giros en dólares estadounidenses.
- Planteamiento de los criterios para cesar relaciones asociadas con giros en dólares estadounidenses.

Procedimientos de Inspección

Giros en dólares estadounidenses

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los giros en dólares estadounidenses, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los giros en dólares estadounidenses. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de giros en dólares estadounidenses del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo. Determine si las políticas abordan lo siguiente:

   - Criterios para permitir que una institución o entidad financiera extranjera expida giros en dólares estadounidenses (por ejemplo: jurisdicción; productos, servicios y mercados objetivo; propósito de la cuenta y actividad prevista; antecedentes del cliente; y otra información disponible).
   - Identificación de transacciones poco habituales (por ejemplo, fraccionamiento de las transacciones o la compra de múltiples giros en dólares estadounidenses numerados en secuencia para el mismo beneficiario).
   - Criterios para cesar la expedición de giros en dólares estadounidenses a través de una institución o entidad financiera extranjera.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de giros en dólares estadounidenses de riesgo más alto.

3. Determine si el sistema del banco para supervisar las cuentas de giros en dólares estadounidenses, detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Obtenga una lista de las cuentas de bancos corresponsales extranjeros en los que se ofrezcan giros en dólares estadounidenses. Revise el volumen, por número y suma en dólares, de las transacciones mensuales de cada cuenta. Determine si la gerencia ha analizado los riesgos de manera adecuada.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades con giros en dólares estadounidenses, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de bancos corresponsales extranjeros en los que se procesen giros en dólares estadounidenses. En la muestra seleccionada, incluya las cuentas con gran volumen de actividad con giros en dólares estadounidenses. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise las transacciones para verificar los giros en dólares estadounidenses numerados en secuencia para el mismo beneficiario o del mismo emisor. Investigue cualquier transacción con giros en dólares estadounidenses sospechosa o poco habitual.
- Revise los contratos y acuerdos del banco con bancos corresponsales extranjeros. Determine si los contratos describen los procedimientos para procesar y compensar giros en dólares estadounidenses.
- Verifique que el banco haya obtenido y controlado la información acerca de las exigencias normativas AML del país de origen de la institución financiera extranjera (por ejemplo, identificación de clientes y presentación de informes de actividades sospechosas).

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con giros en dólares estadounidenses.

Cuentas Empleadas para Pagos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas empleadas para pagos (PTA), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Las instituciones financieras extranjeras utilizan PTA, también conocidas como cuentas "directas" o "de transferencias", para proporcionar a sus clientes el acceso al sistema bancario estadounidense. Algunos bancos estadounidenses, corporaciones que se rigen por la Ley de Organizaciones Bancarias Extranjeras (*Edge Act*) y por un acuerdo con la Junta de Gobernadores del Sistema de Reserva Federal, sucursales estadounidenses y agencias de instituciones financieras extranjeras (colectivamente denominados bancos estadounidenses) ofrecen estas cuentas como un servicio a las instituciones financieras extranjeras. Las autoridades de aplicación de la ley han declarado que el riesgo de lavado de dinero y otras actividades ilícitas es más alto en las PTA que no se controlan de manera adecuada.

Generalmente, una institución financiera extranjera solicita una PTA para sus clientes que desean efectuar transacciones bancarias en los Estados Unidos a través de la cuenta en un banco estadounidense de la institución financiera extranjera. La institución financiera extranjera proporciona a sus clientes, comúnmente denominados "cotitulares de cuentas", cheques que les permiten retirar fondos de la cuenta en el banco estadounidense de la institución financiera extranjera.[169] Los cotitulares de PTA, que pueden ser cientos o miles para una sola cuenta, se convierten todos en firmantes de la cuenta en el banco estadounidense de la institución financiera extranjera. Aunque los clientes de cuentas empleadas para pagos pueden librar cheques y efectuar depósitos en un banco en los Estados Unidos como cualquier otro titular de cuenta, es posible que no estén sujetos de manera directa a las exigencias de apertura de cuentas del banco en los Estados Unidos.

Las actividades de PTA no deben confundirse con las relaciones tradicionales con bancos corresponsales internacionales, en las que una institución financiera extranjera celebra un acuerdo con un banco estadounidense para procesar y efectuar transacciones en nombre de la institución financiera extranjera y sus clientes. Bajo el mencionado acuerdo corresponsal, los clientes de la institución financiera extranjera no tienen acceso directo a la cuenta corresponsal en el banco estadounidense, pero sí realizan negocios a través del banco estadounidense. Este acuerdo difiere significativamente de una PTA con cotitulares de cuentas que tienen acceso directo al banco estadounidense en virtud de su capacidad de efectuar transacciones de manera independiente con el banco estadounidense a través de la PTA.

[169] En este tipo de relación, la institución financiera extranjera se denomina comúnmente "titular principal de cuenta".

Factores de riesgo

Las PTA pueden ser propensas a un riesgo mayor porque los bancos estadounidenses generalmente no implementan las mismas exigencias de debida diligencia para PTA que para los clientes nacionales que desean abrir una cuenta corriente u otro tipo de cuenta. Por ejemplo, algunos bancos estadounidenses simplemente solicitan una copia de las tarjetas de registro de firmas completadas por los clientes de cuentas empleadas para pagos (el cliente de la institución financiera extranjera). Luego, estos bancos estadounidenses procesan miles de cheques de cotitulares de cuentas y otras transacciones, incluidos los depósitos de dinero en efectivo, a través de la PTA de la institución financiera extranjera. En la mayoría de los casos, se hace poco o ningún esfuerzo para obtener o confirmar la información acerca de los cotitulares de cuenta comerciales e individuales que utilizan las PTA.

El uso de las PTA por parte de las instituciones financieras extranjeras, junto a una supervisión inadecuada por parte de los bancos estadounidenses, pueden facilitar las prácticas bancarias cuestionables, incluidos el lavado de dinero y las actividades delictivas relacionadas. La probabilidad de facilitar el lavado de dinero o el financiamiento del terrorismo, las violaciones de la normativa de la OFAC y otros delitos graves aumenta cuando un banco estadounidense no puede identificar y comprender de manera adecuada las transacciones de los usuarios finales (todos o la mayoría de los cuales se encuentran afuera de los Estados Unidos) de su cuenta con un banco corresponsal extranjero. Las PTA que se utilizan para fines ilegales pueden ocasionar a los bancos graves pérdidas financieras en multas y sanciones civiles y penales, embargo o confiscación de bienes dados en garantía, y daños a la reputación.

Mitigación del riesgo

Los bancos estadounidenses que ofrecen servicios de PTA deben desarrollar y mantener políticas, procedimientos y procesos adecuados para protegerse contra el posible uso ilícito de estas cuentas. Como mínimo, las políticas, los procedimientos y los procesos deben permitir a cada banco estadounidense identificar los usuarios finales de su PTA de la institución financiera extranjera y permitirle obtener (o tener la capacidad de obtener a través de un acuerdo con un tercero fiable) sustancialmente la misma información sobre los usuarios finales de la PTA como la que obtiene de sus clientes directos.

Las políticas, los procedimientos y los procesos deben incluir un control de los procesos de la institución financiera extranjera para identificar y supervisar las transacciones de los cotitulares de cuenta y para cumplir con cualquier exigencia normativa y estatutaria AML existente en el país anfitrión y el acuerdo marco de la institución financiera extranjera con el banco estadounidense. Además, los bancos estadounidenses deben contar con procedimientos para supervisar las transacciones efectuadas en las PTA de las instituciones financieras extranjeras.

En un intento de considerar el riesgo inherente a las PTA, los bancos estadounidenses deben contar con un contrato firmado (es decir, un acuerdo marco) que incluya:

- Papeles y responsabilidades de cada parte.
- Límites o restricciones en cuanto a los tipos y las cantidades de transacciones (por ejemplo, depósitos de dinero en efectivo, transferencias de fondos, cobro de cheques).
- Restricciones en cuanto a los tipos de cotitulares de cuentas (por ejemplo, casas de cambio, compañías de financiamiento, emisores de fondos u otras instituciones financieras no bancarias).
- Prohibiciones o restricciones en cuanto a los cotitulares de cuentas con varios niveles.[170]
- Acceso a los documentos internos y auditorías de la institución financiera extranjera concernientes a su actividad de PTA.

Los bancos estadounidenses deben contemplar la posibilidad de cerrar la PTA bajo las siguientes circunstancias:

- Información insuficiente sobre los usuarios finales de la PTA.
- Evidencia de actividad sospechosa sustantiva o continua.
- Incapacidad de garantizar que las PTA no se estén utilizando para el lavado de dinero u otros fines ilícitos.

[170] Una subcuenta se puede subdividir en más subcuentas para diferentes personas.

Procedimientos de Inspección

Cuentas empleadas para pagos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas empleadas para pagos (PTA), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las PTA. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de PTA del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo. Determine si:

   - Los criterios para iniciar relaciones asociadas con PTA con una institución financiera extranjera son adecuados. Los ejemplos de los factores que pueden utilizarse incluyen: jurisdicción; refugios en cuanto al lavado de dinero o secreto bancario; productos, servicios y mercados; propósito; actividad prevista; antecedentes del cliente; propiedad; alta gerencia; acta constitutiva; licencia bancaria; certificado de solvencia y existencia; y demostración de la capacidad operativa de la institución financiera extranjera de supervisar la actividad de cuenta.

   - Se ha obtenido y validado la información adecuada de la institución financiera extranjera sobre la identidad de cualquier persona que tenga autoridad para efectuar transacciones a través de la PTA.

   - Se ha obtenido información y debida diligencia especial de la institución financiera extranjera en cuanto a la fuente y el usufructo de los fondos de personas que tienen autoridad para efectuar transacciones a través de la PTA (por ejemplo, nombre, domicilio, nivel de actividad prevista, lugar de empleo, descripción de la empresa, cuentas relacionadas, identificación de personalidades sujetas a exposición política extranjeras, fuente de los fondos y actas constitutivas).

   - No se han abierto subcuentas antes de que el banco estadounidense haya controlado y aprobado la información del cliente.

   - Las cuentas principales o las subcuentas se pueden cerrar si la información proporcionada al banco es materialmente errónea o está incompleta.

   - El banco puede identificar a todos los firmantes de cada subcuenta.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las PTA.

3. Determine si el sistema de supervisión de las PTA del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Para analizar el volumen de riesgo y determinar si se han asignado recursos adecuados a la actividad de supervisión, procúrese una lista de cuentas de bancos corresponsales extranjeros en los que se ofrezcan PTA y solicite informes de los sistemas para la información de gestión que muestren:

   - La cantidad de subcuentas en cada PTA.
   - El volumen y suma en dólares de las transacciones mensuales de cada subcuenta.

5. Verifique que el banco haya obtenido y controlado la información acerca de las exigencias normativas AML del país de origen de la institución financiera extranjera (por ejemplo, exigencias de identificación de clientes y presentación de informes de actividades sospechosas) y tenga en cuenta estas exigencias al controlar las PTA. Determine si el banco ha garantizado que los acuerdos de subcuentas cumplan con cualquier exigencia normativa y estatutaria AML existente en el país de origen de la institución financiera extranjera.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de PTA, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las PTA. De la muestra, revise los contratos o acuerdos con la institución financiera extranjera. Determine si los contratos o acuerdos:

   - Describen claramente las responsabilidades contractuales tanto del banco estadounidense como de la institución financiera extranjera.
   - Definen los procesos de apertura de PTA y subcuentas, y exigen un control y un proceso de aprobación independientes al abrir la cuenta.
   - Exigen a la institución financiera extranjera que cumpla con sus exigencias AML locales.
   - Restringen la apertura de subcuentas por parte de casas de cambio, compañías de financiamiento, emisores de fondos u otras instituciones financieras no bancarias.
   - Prohíben la existencia de cotitulares de cuentas con varios niveles.
   - Proporcionan controles adecuados sobre los depósitos y las extracciones de dinero en efectivo por parte de los cotitulares de cuentas y garantizan que los informes de transacciones en efectivo se hayan presentado de manera adecuada.
   - Proporcionan límites de dólares para las transacciones de cada cotitular de cuenta que sean coherentes con la actividad prevista de la cuenta.
   - Cuentan con exigencias de documentación que sean coherentes con aquellas utilizadas para la apertura de cuentas nacionales del banco estadounidense.

- Proporcionan al banco estadounidense la capacidad de controlar la información acerca de la identidad de los cotitulares de cuentas (por ejemplo, de manera directa o través de un tercero fiable).
- Exigen a la institución financiera extranjera que supervise las actividades de las subcuentas para detectar actividades sospechosas o poco habituales e informe de los resultados al banco estadounidense.
- Permiten al banco estadounidense, según lo autoricen las leyes locales, llevar a cabo una auditoría de las operaciones de PTA de la institución financiera extranjera y tener acceso a los documentos de PTA.

8. Revise los estados de cuenta principal de PTA. (El inspector debe determinar el plazo en base al tamaño y la complejidad del banco). Los estados de cuenta elegidos deben incluir las transacciones frecuentes y de grandes volúmenes en dólares. Verifique los estados de cuenta según el libro mayor y las conciliaciones bancarias. Tenga en cuenta cualquier envío o depósito de moneda efectuado en el banco estadounidense en nombre de un cotitular de cuenta en particular para verificar el crédito a la subcuenta del cliente.
9. De la muestra seleccionada, revise la información de identificación y transacciones relacionadas de cada cotitular de cuenta durante el período que determine el inspector. Evalúe las transacciones de los cotitulares de PTA. Determine si las transacciones son coherentes con las transacciones previstas o si requieren más investigación. (La muestra debe incluir cotitulares de cuenta con actividad en dólares significativa).
10. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las PTA.

Actividades de Depósitos vía Maletines/Bolsos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de depósitos vía maletines/bolsos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Las actividades de depósitos vía maletines/bolsos implican la utilización de empresas de transporte, de servicios de correo especial (independiente o público) o de agentes referentes empleados por los servicios de correo especial,[171] para transportar moneda, instrumentos monetarios y otros documentos desde afuera de los Estados Unidos a bancos estadounidenses.[172] Otros bancos o personas físicas pueden remitir depósitos vía maletines/bolsos. Los servicios de depósitos vía maletines/bolsos normalmente se ofrecen conjuntamente con servicios de bancos corresponsales extranjeros. Los depósitos vía maletines/bolsos pueden contener pagos de préstamos, transacciones de cuentas corrientes y otros tipos de transacciones. Cada vez más, algunos bancos están utilizando la captura de depósitos remotos (RDC, por sus siglas en inglés), que es un sistema de ejecución de transacciones de depósito que permite reemplazar las actividades de depósitos vía maletines/bolsos. Si desea más información sobre la RDC, consulte la sección del esquema general ampliado sobre Transacciones bancarias electrónicas en las páginas 231 a 235.

Factores de riesgo

Los bancos deben tener en cuenta que con frecuencia se han encontrado en los depósitos vía maletines/bolsos o remesas de cheques recibidos de instituciones financieras extranjeras grandes cantidades de instrumentos monetarios comprados en los Estados Unidos que parecen haber sido estructurados para evitar las exigencias de informe de la BSA. Esto es especialmente válido en el caso de depósitos vía maletines/bolsos y remesas de cheques recibidas de jurisdicciones cuyas estructuras AML son laxas o deficientes. Los instrumentos monetarios involucrados son con frecuencia giros postales, cheques de viajeros y cheques bancarios que usualmente comparten una o más de las siguientes características:

- Los instrumentos se compraron el mismo día o en días consecutivos en diferentes localidades.

---

[171] Los agentes referentes son personas físicas o corporaciones extranjeras, que están obligadas por contrato con el banco estadounidense. Prestan servicios de representación a los clientes del banco en el extranjero a cambio de honorarios. Los servicios pueden ir desde derivar clientes nuevos al banco hasta la administración especial de correo, la obtención y el transporte de documentos, la distribución de folletos y solicitudes o formularios del banco, la escrituración o autenticación de documentos para los clientes y el envío por correo de los fondos de los clientes al banco en los Estados Unidos para su depósito.

[172] Como guía, consulte la sección del esquema general principal, "Informe sobre el transporte internacional de moneda o instrumentos monetarios", en las páginas 162 y 163.

- Están numerados consecutivamente y sus montos son ligeramente inferiores a USD 3.000 o USD 10.000.
- Los espacios donde se deben completar los datos de los beneficiarios se dejan en blanco o se hacen a la misma persona (o solamente a unas pocas personas).
- Contienen poca o ninguna información sobre el comprador.
- Tienen la misma estampilla, símbolo o iniciales.
- Se compran por valores expresados en cifras redondas o por montos repetidos.
- Al depósito de los instrumentos le sigue al poco tiempo una extracción de fondos en forma de transferencia por el mismo valor en dólares.

Mitigación del riesgo

Los bancos deben disponer de políticas, procedimientos y procesos relativos a las actividades de depósitos vía maletines/bolsos que deben:

- Describir los criterios de apertura de una relación de depósitos vía maletines/bolsos con una persona o institución financiera extranjera (por ejemplo, exigencias de debida diligencia de los clientes, tipo de institución o persona, propósito aceptable de la relación).
- Detallar las transacciones aceptables e inaceptables (por ejemplo, instrumentos monetarios cuyos beneficiarios aparecen en blanco, instrumentos monetarios sin firmar, y gran cantidad de instrumentos monetarios con numeración consecutiva).
- Detallar los procedimientos para el procesamiento de los depósitos vía maletines/bolsos, incluidos la responsabilidad de los empleados, controles dobles, exigencias de conciliación y documentación y comprobación de empleados.
- Detallar los procedimientos para el control de actividades poco habituales o sospechosas, incluida la derivación de cualquier inquietud a la gerencia. (Los contenidos de los depósitos vía maletines/bolsos pueden estar sujetos a la exigencia de presentar informes de transacciones en efectivo [CTR], informes sobre el transporte internacional de moneda o instrumentos monetarios [CMIR] e informes de actividades sospechosas [SAR]).
- Dialogar sobre los criterios a emplear para el cierre de las relaciones de depósitos vía maletines/bolsos.

Los factores anteriores deben incluirse en un acuerdo o contrato entre el banco y el correo especial que detalle los servicios que se prestarán y las responsabilidades de las dos partes.

Procedimientos de Inspección

Actividades de depósitos vía maletines/bolsos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de depósitos vía maletines/bolsos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Determine si el banco tiene actividad saliente o entrante de depósitos vía maletines/bolsos y si la actividad se realiza por medio de empresas de transporte o servicios de correo especial.

2. Revise las políticas, los procedimientos, los procesos y cualquier acuerdo contractual relativos a las actividades de depósitos vía maletines/bolsos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de depósitos vía maletines/bolsos y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

3. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de depósitos vía maletines/bolsos.

4. Determine si el sistema de supervisión de las actividades de depósitos vía maletines/bolsos del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Revise la lista de los clientes del banco a los que se les permite utilizar servicios de depósitos vía maletines/bolsos (entrante y saliente). Determine si la gerencia ha analizado el riesgo de los clientes a los que se les permite utilizar este servicio.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de depósitos vía maletines/bolsos, así como de informes de inspecciones previas y de auditoría, seleccione una muestra de los depósitos vía maletines/bolsos diarios para realizar un control. Preferentemente sin previo aviso y durante un período de varios días, no necesariamente consecutivos, observe la apertura de depósitos vía maletines/bolsos y el proceso de obtención de datos sobre los elementos incluidos en la muestra de depósitos vía maletines/bolsos entrantes, y observe la preparación de los depósitos vía maletines/bolsos salientes. Revise los registros y los contenidos de los depósitos vía

maletines/bolsos en busca de moneda, instrumentos monetarios,[173] valores al portador, tarjetas prepagadas, piedras preciosas, trabajos artísticos, sustancias ilegales, artículos de contrabando u otros elementos que no deberían aparecer normalmente en un depósito vía maletines/bolsos del banco.

8. Si el correo especial o el agente referente que trabaja para este, tiene una cuenta en el banco, revise una muestra adecuada de la actividad de su cuenta.

9. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con los depósitos vía maletines/bolsos.

---

[173] Consulte los procedimientos de inspección de la sección principal, “Informes sobre el transporte internacional de moneda o instrumentos monetarios”, en las páginas 162 y 163, como guía.

Banca Electrónica: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los clientes de banca electrónica (transacciones bancarias electrónicas), incluida la actividad de captura de depósitos remotos (RDC), y la capacidad de la gerencia para implementar sistemas de supervisión e informe eficaces.*

Los sistemas de transacciones bancarias electrónicas, que proporcionan la entrega electrónica de productos bancarios a los clientes, incluyen las transacciones por cajero automático (ATM); la apertura de cuentas por Internet; las transacciones bancarias por Internet; y las transacciones bancarias telefónicas. Por ejemplo, las tarjetas de crédito, las cuentas de depósito, los préstamos hipotecarios y las transferencias de fondos pueden iniciarse a través de Internet, sin contacto directo. La gerencia debe reconocer ésta como un área de un posible riesgo más alto y elaborar políticas, procedimientos y procesos para identificar a clientes y supervisar áreas específicas de las operaciones bancarias. Consulte la sección del esquema general principal, "Programa de identificación de clientes" (CIP), en las páginas 65 a 68, como guía. Más información sobre las transacciones bancarias electrónicas está disponible en *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[174]

Factores de riesgo

Los bancos deben asegurar que sus sistemas de supervisión detecten de manera adecuada las transacciones que se realicen electrónicamente. Como en cualquier cuenta, deben estar alerta a toda anomalía que presente la cuenta. Las señales de advertencia pueden incluir la velocidad con que ingresan fondos a la cuenta o, en el caso de los cajeros automáticos, el número de tarjetas de débito asociadas a la cuenta.

Las cuentas abiertas sin contacto directo pueden implicar mayor riesgo de lavado de dinero y financiamiento del terrorismo, por las siguientes razones:

- Es más difícil verificar positivamente la identidad de la persona.
- El cliente puede estar fuera del área geográfica o país que es el objetivo del banco.
- El cliente puede percibir las transacciones como menos transparentes.
- Las transacciones son instantáneas.
- Pueden ser utilizadas por una empresa "pantalla" o terceros desconocidos.

[174] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Mitigación del riesgo

Los bancos deben establecer supervisión, identificación e informe BSA/AML de actividades sospechosas y poco habituales que ocurran a través de sistemas de transacciones bancarias electrónicas. Los sistemas para la información de gestión útiles para detectar las actividades poco habituales en cuentas de mayor riesgo incluyen los informes de actividad de cajeros automáticos, informes de transferencias de fondos, informes de actividad de cuentas nuevas, informes de cambio de dirección de Internet, informes de direcciones de Protocolo de Internet (IP) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, direcciones, números telefónicos, direcciones de correo electrónico y números de identificación tributaria comunes). Para determinar el nivel de supervisión que requiere una cuenta, uno de los factores que los bancos deberían considerar es la forma en que fue abierta la cuenta. Los bancos que se dedican a realizar transacciones bancarias a través de Internet deben contar con métodos confiables y eficaces para legitimar la identidad de los clientes cuando se abren cuentas en línea y deben establecer políticas que determinen cuándo los clientes deberán abrir cuentas mediante contacto directo.[175] Los bancos pueden también imponer otros controles, como establecer límites a las transacciones en dólares de montos elevados, de manera que se requiera una intervención manual para superar el límite preestablecido.

Captura de depósitos remotos

La captura de depósitos remotos (RDC) es un sistema de ejecución de transacciones de depósito que ha aumentado la eficacia del procesamiento de cheques e instrumentos monetarios (por ejemplo, cheques de viajero o giros postales). En términos más amplios, la RDC les permite a los clientes de un banco escanear un cheque o un instrumento monetario, y transmitir posteriormente la imagen escaneada o digitalizada a la institución. Las actividades de escaneado y transmisión ocurren en ubicaciones remotas que incluyen las sucursales del banco, los ATM, los bancos corresponsales nacionales y extranjeros, y las ubicaciones permitidas o controladas por los clientes minoristas o comerciales. Al eliminar las transacciones en persona, la RDC permite disminuir el costo y el volumen de papel asociados con el envío por correo o el depósito físico de elementos. Además, la RDC es compatible con los productos bancarios nuevos y existentes, y posibilita un mejor acceso de los clientes a sus depósitos.

El 14 de Enero de 2009, el FFIEC publicó una guía denominada *Risk Management of Remote Deposit Capture* (Gestión del riesgo de la captura de depósitos remotos) que cubre los componentes fundamentales de la gestión del riesgo de la RDC: la identificación, el análisis y la mitigación del riesgo. Incluye un desarrollo exhaustivo de los factores de riesgo de la RDC y los elementos de mitigación. Consulte www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.

---

[175] Para obtener más información, consulte *Authentication in an Internet Banking Environment* (Autenticación en un entorno bancario en Internet), publicado por el FFIEC el 13 de OctubreOctubre de 2005.

Factores de riesgo

La RDC puede exponer a los bancos a diferentes riesgos, entre ellos, de lavado de dinero, fraude y seguridad de la información. Los documentos fraudulentos, numerados en secuencia o físicamente modificados, en especial los cheques de viajero y los giros postales, son más difíciles de detectar cuando se envían mediante la RDC y no son revisados por una persona calificada. Los bancos pueden enfrentar desafíos al tratar de controlar o conocer la ubicación del equipo de RDC, debido a que el equipo se puede trasportar rápidamente de una jurisdicción a otra. Este desafío aumenta en la medida en que cada vez más compañías de servicios en moneda extranjera y bancos corresponsales extranjeros usan los servicios de RDC para reemplazar las actividades de depósitos vía maletines/bolsos y ciertas actividades de procesamiento y compensación de instrumentos. Los controles inadecuados pueden derivar en alteraciones intencionales o accidentales de los datos del elemento de depósito, el reenvío de un archivo de datos o la presentación duplicada de cheques e imágenes en una o más instituciones financieras. Además, los elementos de depósito originales generalmente no son enviados a los bancos, sino que, por el contrario, quedan en poder del cliente o del prestador de servicios del cliente. En consecuencia, pueden aumentar los problemas de integridad, seguridad de los datos y gestión de registros.

Los clientes de riesgo más alto se pueden definir según la industria, la incidencia de fraude u otros criterios. Algunos ejemplos de partes de riesgo más alto incluyen los procesadores de pago en línea, ciertos servicios de reparación de crédito, ciertas compañías de solicitud de pedidos por vía telefónica o por correo, las operaciones de apuestas en línea, las empresas instaladas en el exterior y las empresas de entretenimiento para adultos.

Mitigación del riesgo

La gerencia debe desarrollar políticas, procedimientos y procesos adecuados para mitigar los riesgos asociados con los servicios de RDC y para supervisar actividades sospechosas o poco habituales de manera eficaz. Los ejemplos de medidas apropiadas para mitigar el riesgo incluyen:

- Identificar y analizar exhaustivamente el riesgo de RDC antes de su implementación. La alta gerencia debe identificar los riesgos de BSA/AML, operativos, de seguridad de la información, de cumplimiento, legales y aquellos que comprometen la reputación. Según el tamaño y la complejidad del banco, este proceso de análisis de riesgos integral debe incluir a miembros del personal de las áreas de BSA/AML, tecnología de la información y seguridad, operaciones de depósito, tesoro o administración del dinero resultante de las ventas al contado, continuidad empresarial, auditoría, cumplimiento, contabilidad y asuntos legales.

- Implementar adecuadamente la EDD y la CDD de los clientes.

- Crear parámetros basados en el riesgo que se puedan usar para realizar controles de la aptitud de la RDC para los clientes. Los parámetros pueden incluir una lista de industrias aceptables, criterios de colocación estandarizados (por ejemplo,

antecedentes de crédito, estados financieros, y estructura de propiedad comercial) y otros factores de riesgo (procesos de gestión de riesgos del cliente, ubicación geográfica y base de clientes). Cuando el nivel de riesgo lo justifique, el personal debe considerar realizar una visita a la ubicación física del cliente como parte del control de aptitud. Durantes estas visitas, deben evaluarse los controles operativos y los procesos de gestión de riesgos del cliente.

- Llevar a cabo la debida diligencia del proveedor cuando los bancos utilicen un prestador de servicios para las actividades de RDC. La gerencia debe garantizar la implementación de procesos de gestión de proveedores sólidos.

- Obtener la actividad de cuenta prevista del cliente de RDC, como el volumen de transacciones de RDC previsto, el volumen en dólares y el tipo (por ejemplo, cheques de nómina, cheques de terceros o cheques de viajero), compararla con la actividad real y corregir las desviaciones significativas. Comparar la actividad prevista con el tipo de actividad comercial a fin de asegurar que sea razonable y coherente.

- Establecer o modificar los límites de las transacciones mediante RDC para los clientes.

- Desarrollar contratos correctamente estructurados que identifiquen claramente el papel, las responsabilidades y las obligaciones de cada parte, y que detallen los procedimientos de conservación de registros para los datos de RDC. Estos procedimientos deben incluir las expectativas de seguridad física y lógica para el acceso, la transmisión, el almacenamiento y la eliminación definitiva de los documentos originales. El contrato también debe estipular la responsabilidad del cliente de asegurar adecuadamente el equipo de RDC y evitar su uso indebido, incluido el establecimiento de controles eficaces de seguridad del equipo (por ejemplo, contraseñas, acceso de doble control). Asimismo, los contratos deben incluir la obligación de los clientes de RDC de proporcionar los documentos originales al banco para facilitar las investigaciones relacionadas con las transacciones poco habituales o las transmisiones de mala calidad, o para resolver conflictos. Los contratos deben detallar claramente la autoridad del banco para implementar controles internos específicos, realizar auditorías o finalizar la relación de RDC.

- Implementar una supervisión o un control adicional cuando haya cambios significativos en el tipo o el volumen de las transacciones, o en los criterios de colocación, tipo de clientela, los procesos de gestión de riesgos de los clientes o la ubicación geográfica de los que el banco se haya valido cuando estableció los servicios de RDC.

- Asegurar que los clientes de RDC reciban la capacitación adecuada. Dicha capacitación debe incluir la documentación que cubra cuestiones como los procedimientos y las operaciones de rutina, la presentación duplicada y la resolución de problemas.

- Utilizar capacidad optima de supervisión y acumulación facilitadas por los datos digitalizados.

- Según corresponda, utilizar la tecnología para minimizar los errores (por ejemplo, el uso del franqueo para imprimir o identificar un depósito que está siendo procesado).[176]

[176] El franqueo involucra la impresión o el estampado de frases como "Procesado" o "Procesado electrónicamente" en el frente del cheque original. Este proceso se utiliza como un indicador de que el cheque impreso ya ha sido procesado electrónicamente y, en consecuencia, ya no debe depositarse físicamente.

Procedimientos de Inspección

Banca electrónica

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los clientes de banca electrónica (transacciones bancarias electrónicas), incluida la actividad de captura de depósitos remotos (RDC), y la capacidad de la gerencia para implementar sistemas de supervisión e informe eficaces.*

1. Revise las políticas, los procedimientos y los procesos relacionados con transacciones bancarias electrónicas, incluida la actividad de RDC según sea pertinente. Evalúe la aptitud de las políticas, los procedimientos y los procesos con relación con las actividades de transacciones bancarias electrónicas del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de transacciones bancarias electrónicas de riesgo más alto.

3. Determine si el sistema del banco para supervisar las transacciones bancarias electrónicas, incluyendo las actividades de RDC según sea pertinente, para detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de transacciones bancarias electrónicas, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de transacciones bancarias electrónicas. De la muestra seleccionada, lleve a cabo los siguientes procedimientos:

   - Revise la documentación de apertura de la cuenta, incluida la del CIP, la debida diligencia continua de los clientes y los antecedentes de transacciones.
   - Compare la actividad prevista con la actividad real.
   - Determine si la actividad es coherente con el tipo de negocio del cliente. Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a la relacion asociada con transacciones bancarias electrónicas.

Transferencias de Fondos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transferencias de fondos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales de las transferencias de fondos para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

En los Estados Unidos, los sistemas de pago consisten en numerosos intermediarios financieros, empresas de servicios financieros y empresas no bancarias que generan, procesan y distribuyen pagos. La expansión nacional e internacional de la industria de operaciones bancarias y los servicios financieros no bancarios ha intensificado la importancia de las transferencias electrónicas de fondos, como las transferencias de fondos a través de sistemas de pago al por mayor. Más información sobre los tipos de sistemas de pago al por mayor está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[177]

Servicios de transferencia de fondos

La gran mayoría del valor de las transferencias o los pagos efectuados en dólares estadounidenses en los Estados Unidos se procesa en última instancia a través de sistemas de pago al por mayor, que por lo general manejan transacciones de mucho valor entre bancos. Los bancos realizan estas transferencias tanto a nombre propio como en beneficio de otros prestadores de servicios financieros y clientes del banco, ya sean corporaciones o particulares.

Los sistemas de transferencia al por menor relacionados facilitan las transacciones dado que incluyen cámaras de compensación automática (ACH); cajeros automáticos (ATM); sistemas de puntos de venta (POS); pago telefónico de cuentas; sistemas *home banking;* y tarjetas de crédito, de débito, y prepagadas. Los que inician la mayoría de estas transacciones al por menor son los clientes, en lugar de los bancos y las corporaciones. Estas transacciones individuales pueden entonces procesarse por lotes para formar transferencias al por mayor más grandes, que son el centro de interés en esta sección.

Los dos principales sistemas nacionales de pago al por mayor de transferencias de fondos interbancarias son los Servicios de fondos Fedwire (Fedwire®)[178] y el Sistema de pagos interbancarios por cámara de compensación (CHIPS).[179] La mayor parte del valor en dólares de estos pagos se origina electrónicamente para hacer pagos de alto valor en los

[177] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[178] Fedwire® es una marca registrada de servicio de los Bancos de la Reserva Federal. Consulte www.frbservices.org/fedwire/index.html para obtener más información.

[179] CHIPS es un sistema privado de liquidación multilateral que pertenece y es operado por The Clearing House Payments Co., LLC.

que el tiempo es un factor clave, como liquidar compras interbancarias y vender fondos federales, liquidar transacciones de cambio de moneda extranjera, desembolsar o pagar préstamos, liquidar transacciones de bienes inmuebles u otras transacciones del mercado financiero; y la compra, venta o financiación de transacciones de valores. Las personas que utilizan Fedwire y CHIPS facilitan estas transacciones en su nombre y en nombre de sus clientes, incluyendo instituciones financieras no bancarias, empresas comerciales, y bancos corresponsales que no tienen acceso directo. Estructuralmente, hay dos componentes de las transferencias de fondos.

La estructura de las transferencias de fondos posee dos componentes: las instrucciones, que contienen información del remitente y el receptor de los fondos, y el movimiento o transferencia real de los fondos. Las instrucciones pueden enviarse por diferentes vías, por ejemplo accediendo electrónicamente a las redes operadas por los sistemas de pago Fedwire o CHIPS; accediendo a los sistemas de telecomunicaciones financieras, como la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT); o por correo electrónico, fax, teléfono o télex. Se utilizan Fedwire y CHIPS para facilitar las transferencias en dólares estadounidenses entre dos extremos nacionales o de la porción en dólares estadounidenses de las transacciones internacionales. SWIFT es un servicio de mensajería internacional que se utiliza para transmitir las instrucciones de pago de la gran mayoría de transacciones internacionales interbancarias, que pueden estar denominadas en muchos tipos de moneda.

Fedwire

El sistema Fedwire es operado por los Bancos de la Reserva Federal y le permite a todo participante transferir fondos desde su cuenta principal en el Banco de la Reserva Federal a cualquier otra cuenta principal de cualquier otro banco.[180] El pago a través de Fedwire es definitivo e irrevocable cuando el Banco de la Reserva Federal acredita el monto de la orden de pago en la cuenta principal que el banco receptor tiene en el Banco de la Reserva Federal, o envía una notificación al banco receptor, según lo que ocurra primero. Aunque los participantes del sistema Fedwire no corren el riesgo de liquidación, pueden estar expuestos a otros riesgos, como errores, omisiones y fraude.

---

[180] Una entidad que cumple con los requisitos para mantener una cuenta principal en la Reserva Federal generalmente cumple con los requisitos para participar en el Servicio de Fondos Fedwire. Estos participantes incluyen:

- Instituciones de depósito.
- Agencias y sucursales estadounidenses de bancos extranjeros.
- Bancos miembros del Sistema de la Reserva Federal.
- El Tesoro de los EE. UU y cualquier entidad específicamente autorizada por ley federal para utilizar los Bancos de la Reserva Federal como agentes fiscales o de depósito.
- Entidades designadas por el Secretario del Tesoro.
- Los bancos centrales extranjeros, autoridades monetarias extranjeras, gobiernos extranjeros, y ciertas organizaciones internacionales.
- Cualquier otra entidad autorizada por el Banco de la Reserva Federal para utilizar el Servicio de Fondos Fedwire.

Los participantes pueden acceder al sistema Fedwire a través de los siguientes tres métodos:

- Interfaz directa de computador (sistema FedLine directo).
- Acceso a Internet a través de una red privada virtual a aplicaciones basadas en la Web (*FedLine Advantage*).
- Acceso autónomo o a través de una línea telefónica a un sitio de operaciones de un Banco de la Reserva Federal.

CHIPS

CHIPS es un sistema de pagos multilateral administrado por particulares que opera en tiempo real y que se utiliza generalmente para el pago de grandes montos en dólares. El sistema CHIPS es de propiedad de los bancos, y toda organización bancaria con presencia estadounidense regulada puede participar del sistema. Los bancos utilizan CHIPS para la liquidación tanto de transacciones interbancarias como de clientes, incluidos, por ejemplo, los pagos asociados con transacciones comerciales, los préstamos bancarios y las transacciones de valores. CHIPS también desempeña un papel importante en la liquidación de pagos en dólares relacionados con las transacciones internacionales, como el cambio de moneda extranjera, las transacciones comerciales internacionales y las inversiones en el extranjero.

Banco de liquidación vinculada continua (CLS)

El Banco de CLS es un banco con un propósito especial de sector privado que liquida de manera simultánea ambas obligaciones de pago que surgen de una sola transacción de cambio de moneda extranjera. El pago de CLS frente al modelo de la liquidación de pago garantiza que una parte del pago de una transacción de cambio de moneda extranjera se liquide si y sólo si la parte de pago correspondiente también se liquida, eliminando el riesgo de la liquidación de cambio de moneda extranjera que surge cuando cada parte de la transacción de moneda extranjera se liquida por separado. La CLS es propiedad de instituciones financieras mundiales a través de la posesión de acciones en CLS Group Holdings AG, una compañía suiza que es la sociedad de control final para el Banco de CLS. Actualmente, el Banco de CLS liquida instrucciones de pago para transacciones de cambio de moneda extranjera en 17 divisas y se espera que con el tiempo incluya más divisas.

SWIFT

La red SWIFT no es un sistema de pagos sino una infraestructura de mensajería, que proporciona a los usuarios un vínculo privado de comunicaciones internacionales entre ellos mismos. Los movimientos de fondos reales (pagos) se realizan a través de las relaciones bancarias corresponsales, Fedwire o CHIPS. El movimiento de los pagos denominados en monedas diferentes se produce mediante las relaciones bancarias corresponsales o los sistemas de transferencias de fondos existentes en el país pertinente. Además de las transferencias de fondos del banco y del cliente, se utiliza la SWIFT para transmitir confirmaciones de cambio de moneda extranjera, confirmaciones de ingresos de débitos y créditos, estados de cuenta, cobros y créditos documentados.

Pagos de cobertura

Una transferencia de fondos típica involucra a un remitente que le indica a su banco (el banco del remitente) que efectúe un pago en la cuenta de un beneficiario en el banco del beneficiario. Un pago de cobertura ocurre cuando el banco del remitente y el banco del beneficiario no tienen una relación que les permita realizar el pago directamente. En dicho caso, el banco del remitente le indica al banco del beneficiario que efectúe el pago y notifica que la transmisión de fondos para "cubrir" la obligación creada por la orden de pago se ha dispuesto a través de cuentas corresponsales a uno o más bancos intermediarios.

Los pagos de cobertura transnacionales generalmente involucran varios bancos en diversas jurisdicciones. Por lo general, para las transacciones en dólares estadounidenses, los bancos intermediarios son bancos estadounidenses que mantienen relaciones de banca corresponsal con los bancos no estadounidenses de los remitentes y los beneficiarios. En el pasado, los protocolos de mensaje de SWIFT permitían que los pagos de cobertura transnacionales se realizaran mediante el uso de formatos de mensaje simultáneos e independientes:

- el MT 103: orden de pago del banco del remitente al banco del beneficiario con información identificativa del remitente y el beneficiario; y
- el MT 202: órdenes de pago de banco a banco mediante las que se indica a los bancos intermediarios que "cubran" la obligación de pago del banco del remitente al banco del beneficiario.

A fin de evitar la falta de transparencia, SWIFT adoptó un nuevo formato de mensaje para los pagos de cobertura (el MT 202 COV) que contiene campos obligatorios para rellenar con información del remitente y el beneficiario. Vigente desde el 21 de Noviembre de 2009, el MT 202 COV es obligatorio para todo pago de banco a banco que tenga asociado un MT 103. El MT 202 COV proporciona a los bancos intermediarios información adicional sobre el remitente y el beneficiario para ejecutar la revisión de sanciones y la supervisión de las actividades sospechosas.[181] La incorporación del MT 202 COV no altera las obligaciones de OFAC o BSA/AML de un banco estadounidense.

El formato MT 202 sigue estando disponible para las transferencias de fondos de banco a banco que no tengan un mensaje MT 103 asociado. Si desea obtener información adicional sobre la transparencia en los pagos de cobertura, consulte *Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers* (Transparencia y cumplimiento de las organizaciones bancarias estadounidenses que realizan transferencias de fondos transnacionales), del 18 de Diciembre de 2009, disponible en el sitio web de las agencias bancarias federales.

---

[181] En el sitio web de SWIFT, www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2009/Newstandardsforcoverpayments.page, se puede encontrar información adicional sobre los detalles del formato MT 202 COV

Sistemas informales de transferencia de valor

Por sistema informal de transferencia de valor (IVTS, por sus siglas en inglés) (por ejemplo, los hawalas) se entiende el sistema de transferencia de moneda o valor que opera informalmente para transferir dinero como negocio.[182] En los países que carecen de un sector financiero estable o que tienen grandes áreas no atendidas por bancos formales, el sistema IVTS puede ser el único método para realizar transacciones financieras. Las personas que viven en los Estados Unidos también pueden utilizar IVTS para transferir fondos hacia sus países de origen.

Transacciones pagaderas mediante presentación de identificación apropiada

Un tipo de transacción de transferencia de fondos que implica un riesgo particular es el servicio de transacciones pagaderas mediante presentación de identificación apropiada (PUPID). Las transacciones PUPID son transferencias de fondos en las que no existe una cuenta específica para depositar los fondos y el beneficiario de los fondos no es cliente del banco. Por ejemplo, una persona física puede transferir fondos a un familiar o a una persona que no tenga una relación de cuenta con el banco que recibe la transferencia de fondos. En este caso, el banco beneficiario puede colocar los fondos que ingresan en una cuenta puente o de tránsito y, en última instancia, liberar los fondos cuando la persona presente pruebas respecto a su identidad. En algunos casos, los bancos autorizan a entidades que no son clientes a iniciar transacciones PUPID. Estas transacciones se consideran de un riesgo extremadamente alto y requieren controles estrictos.

Factores de riesgo

Las transferencias de fondos pueden presentar un aumento en el grado de riesgo, que depende de factores como la cantidad y volumen en dólares de las transacciones, la ubicación geográfica de remitentes y beneficiarios, y de si el remitente o el beneficiario es cliente del banco. El tamaño y la complejidad de la operación de un banco, y el origen y el destino de los fondos que están siendo transferidos determinarán qué tipo de sistema de transferencia de fondos utilizará el banco. La gran mayoría de las instrucciones de

[182] Las fuentes de información sobre IVTS incluyen:

- Asesoría 33 de la FinCEN, *Informal Value Transfer Systems* (Sistemas Informales de Transferencia de Valor), de Marzo de 2003.
- *Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act* (Informe al Congreso de los sistemas informales de transferencia de valores del Tesoro de los Estados Unidos según la Sección 359 de la Ley *Patriot*), de Noviembre 2002.
- Grupo de Acción Financiera en Contra del Lavado de Dinero (FATF), *Interpretative Note to Special Recommendation VI: Alternative Remittance* (Nota interpretativa a la Recomendación Especial VI: Remesas alternativas), de Junio de 2003.
- FATF, *Combating the Abuse of Alternative Remittance Systems, International Best Practices* (Lucha contra el abuso de los sistemas de remesas alternativas, Mejores prácticas internacionales), de Octubre de 2002.

transferencia de fondos se envía electrónicamente; sin embargo, los inspectores deben ser conscientes de que las instrucciones físicas se pueden transmitir por otras vías informales, como las descritas anteriormente.

Los pagos de cobertura realizados a través de SWIFT plantean un riesgo adicional para cualquier banco intermediario que no reciba un MT 103 o un MT 202 COV correctamente completo, en el que se identifique el remitente y el beneficiario de la transferencia de fondos. Sin estos datos, el banco intermediario no puede supervisar o filtrar la información de pago. Esta falta de transparencia limita la capacidad del banco intermediario estadounidense para analizar y gestionar adecuadamente el riesgo asociado con las operaciones de compensación y cuentas corresponsales, supervisar las actividades sospechosas y corroborar el cumplimiento con la OFAC.

Los IVTS plantean un problema serio porque pueden burlar el sistema formal. La ausencia de exigencias de gestión de registros junto a la falta de identificación de quienes participan en el sistema IVTS puede atraer a lavadores de dinero y terroristas. Los IVTS también pueden implicar mayor riesgo BSA/AML porque permiten evadir los controles internos y la supervisión establecidos en el entorno bancario formal. Los mandantes que operan sistemas IVTS con frecuencia utilizan los bancos para liquidar cuentas.

Los riesgos que implican las transacciones PUPID para los bancos beneficiarios son similares a los de otras actividades en las que los bancos hacen negocios con quienes no son clientes. Sin embargo, los riesgos son mayores en las transacciones PUPID si el banco permite que una persona que no es cliente acceda al sistema de transferencias de fondos proporcionando mínima o ninguna información de identidad. Los bancos que permiten a quienes no son clientes transferir fondos utilizando el servicio PUPID ponen en riesgo significativo tanto al banco beneficiario como al banco en donde se originó la transferencia. En estas situaciones, los dos bancos tienen mínima información sobre la identidad tanto del remitente como del beneficiario o carecen de ella por completo.

Mitigación del riesgo

Las transferencias de fondos se pueden utilizar en las fases de colocación, transformación e integración del lavado de dinero. Las transferencias de fondos compradas con moneda son un ejemplo de la etapa de colocación. Es más difícil para los bancos detectar actividad poco habitual en las etapas de transformación e integración porque las transacciones pueden parecer legítimas. En muchos casos, los bancos no participan en la colocación de los fondos o en la integración final, sino únicamente en la transformación de las transacciones. Los bancos deben tener en cuenta las tres fases del lavado de dinero cuando evalúan o analizan los riesgos de la transferencia de fondos.

Los bancos necesitan establecer políticas, procedimientos y procesos responsables para gestionar los riesgos BSA/AML que presentan sus actividades de transferencia de fondos. Dichas políticas pueden incluir más que exigencias normativas mínimas en cuanto a la gestión de registros y expandirse para cubrir la OFAC. Las políticas, los procedimientos y los procesos de las transferencias de fondos deben ocuparse de todas las actividades de bancos corresponsales extranjeros, incluidas las transacciones en las que las sucursales y agencias estadounidenses de bancos extranjeros sean intermediarias para sus oficinas centrales.

La obtención de información de CDD es importante para mitigar el riesgo en la prestación de servicios de transferencia de fondos. Debido al carácter de las transferencias de fondos, es fundamental contar con políticas, procedimientos y procesos CDD eficaces y adecuados para detectar actividades sospechosas y poco habituales. Es igualmente importante disponer de un sistema de informe y supervisión de actividades sospechosas eficaz en función del riesgo. Tanto si este sistema de informe y supervisión es automatizado como si es manual, debe ser suficiente para detectar patrones y tendencias sospechosos que por lo general se asocian con el lavado de dinero.

Las instituciones deben tener procesos para gestionar las relaciones de banca corresponsal de acuerdo con la sección 312 de la Ley PATRIOTA de EE. UU. y los reglamentos pertinentes (31 CFR 103.176). La debida diligencia de la banca corresponsal debe tener en cuenta las prácticas del banco corresponsal con relación a la transferencia de fondos a través del banco estadounidense.

Los bancos estadounidenses pueden mitigar el riesgo asociado con los pagos de cobertura al gestionar relaciones de banca corresponsal, al cumplir con las mejores prácticas de The Clearing House Payments Co., LLC y el Grupo Wolfsberg (tema desarrollado a continuación) y las normas de SWIFT para el envío de mensajes, y al realizar la correcta revisión y supervisión de las transacciones.

En Mayo de 2009, el Comité de Supervisión Bancaria de Basilea publicó un documento sobre los mensajes de pagos cobertura de transnacionales (Documento sobre los pagos de cobertura del BIS).[183] El Documento sobre los pagos de cobertura del BIS admitía el aumento de la transparencia y recomendaba a todos los bancos involucrados en las transacciones de pagos internacionales que cumplieran con las normas de mensajes desarrolladas por The Clearing House Payments Co., LLC y el Grupo Wolfsberg en 2007. Estas son:

- Las instituciones bancarias no deben omitir, eliminar o alterar la información en las órdenes o los mensajes de pago con el fin de evitar la detección de dicha información por parte de cualquier otra institución financiera en el proceso de pago.
- Las instituciones financieras no deben utilizar los mensajes de pago particulares con el fin de evitar la detección de información por parte de cualquier otra institución en el proceso de pago.
- Sujeto a todas las leyes pertinentes, las instituciones financieras deben cooperar tanto como sea viable con otras instituciones financieras en el proceso de pago cuando se les solicite que proporcionen información acerca de las partes involucradas.

[183] Comité de Supervisión Bancaria de Basilea, *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* (Debida diligencia y transparencia relacionadas con los mensajes de pagos de cobertura correspondientes a las transferencias electrónicas transnacionales, disponibles en www.bis.org/publ/bcbs154.htm. Además, durante el mes de Agosto de 2009, el comité, junto con The Clearing House Payments Co., LLC, publicó preguntas y respuestas con el objeto de aumentar la comprensión de MT 202 COV.

- Las instituciones financieras deben recomendar enfáticamente a sus bancos corresponsales que respeten estos principios.

Asimismo, los procesos eficaces de supervisión de los pagos de cobertura incluyen:

- La supervisión de las transferencias de fondos procesadas mediante sistemas automatizados con el fin de identificar actividades sospechosas. Esta supervisión puede realizarse después del procesamiento de las transferencias, en forma automatizada, y se puede utilizar un enfoque basado en el riesgo. El MT 202 COV proporciona a los bancos intermediarios información útil, que se puede filtrar usando los factores de riesgo desarrollados por el banco intermediario. El proceso de supervisión puede ser similar al de los pagos mediante MT 103.

- Dado el volumen de los mensajes y la información de los grandes bancos intermediarios estadounidenses, es posible que el control manual de cada orden de pago no sea factible o eficaz. Sin embargo, los bancos intermediarios deben tener, como parte de sus procesos de supervisión, un método basado en el riesgo para identificar los campos incompletos o los campos con información sin sentido. Los bancos estadounidenses que participan en el procesamiento de pagos de cobertura deben tener políticas para abordar tales circunstancias, incluidas aquellas que involucran sistemas distintos de SWIFT.

Los bancos remitentes y beneficiarios deben establecer políticas, procedimientos y procesos adecuados para las actividades PUPID que incluyan:

- Especificación del tipo de identificación que se considera aceptable.

- Mantener documentación de personas físicas que sea consistente con las políticas de conservación de registros del banco.

- Delimitación de los empleados del banco que pueden realizar transacciones PUPID.

- Fijación de límites en la cantidad de fondos que pueden ser transferidos desde y hacia los bancos para quienes no son clientes (incluyendo el tipo de fondos que se acepta (es decir, moneda o cheque oficial) de parte del banco remitente.

- Supervisión e informe de actividades sospechosas.

- Escrutinio especial para transferencias realizadas desde y hacia ciertas jurisdicciones.

- Identificación de los métodos de desembolso (es decir, en moneda o cheque oficial) de los fondos provenientes de un banco beneficiario.

Procedimientos de Inspección

Transferencias de fondos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las transferencias de fondos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales de las transferencias de fondos para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las transferencias de fondos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de transferencias de fondos del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las actividades de transferencias de fondos.

3. Evalúe los riesgos del banco relacionados con las actividades de transferencias de fondos al analizar la frecuencia y el volumen en dólares de las transferencias de fondos, las jurisdicciones y el papel del banco en el proceso de transferencia de fondos (por ejemplo, si es el banco del remitente, del intermediario o del beneficiario). Estos factores deben evaluarse con relación al tamaño del banco, su ubicación y la naturaleza de las relaciones de las cuentas corresponsales y los clientes.

4. Determine si existe un rastro de auditoría respecto a las actividades de transferencias de fondos. Determine si se dispone de una división de responsabilidades u otros controles compensatorios adecuados para garantizar la autorización adecuada para enviar y recibir transferencias de fondos, y corregir las imputaciones a cuentas.

5. Determine si el sistema del banco para supervisar las transferencias de fondos e informar sobre las actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de supervisión e informe de actividades sospechosas incluyen:

   - Transferencias de fondos adquiridas con dinero en efectivo.
   - Transacciones en las que el banco actúe como intermediario.
   - Todos los formatos de mensaje de SWIFT, incluidos MT 103, MT 202 y MT 202 COV.
   - Transacciones en las que el banco remite o recibe transferencias de fondos de instituciones financieras extranjeras, particularmente desde o hacia jurisdicciones con leyes de secreto y privacidad estrictas, o aquellas identificadas como de riesgo más alto.

- Depósitos de dinero en efectivo frecuentes o transferencias de fondos y las transferencias posteriores, particularmente a una institución más grande o fuera del país.

6. Revise los procedimientos del banco para realizar las transferencias de fondos transnacionales:

   - Determine si los procesos del banco para la debida diligencia de bancos corresponsales extranjeros, según se estipula en la sección 312 de la Ley PATRIOTA de EE. UU. y los reglamentos pertinentes, incluyen la revisión y la evaluación de las prácticas de transparencia de los corresponsales del banco involucrados en las transferencias de fondos transnacionales a través del banco (por ejemplo, si los corresponsales están utilizando correctamente el formato de mensaje MT 202 COV).

   - Según corresponda y en tanto no se haya hecho hasta el momento, revise los procedimientos del banco para garantizar el cumplimiento de la *Travel Rule*, incluido el uso adecuado del formato MT 202 COV.

   - Evalúe las políticas del banco para cooperar con sus corresponsales cuando estos le soliciten al banco que proporcione información acerca de las partes involucradas en las transferencias de fondos.

   - Evalúe la aptitud de los procedimientos del banco para abordar las instancias aisladas y reiteradas donde la información de pago proporcionada por un corresponsal falta, claramente carece de sentido, está incompleta o es sospechosa.

7. Determine los procedimientos del banco para transacciones pagaderas mediante presentación de identificación apropiada (PUPID).

   - Banco beneficiario: determine cómo desembolsa el banco los ingresos (es decir, mediante dinero en efectivo o cheque oficial).

   - Banco remitente: determine si el banco admite las transferencias de fondos PUPID a quienes no son clientes. De ser así, determine el tipo de fondos aceptados (es decir, en dinero en efectivo o cheque oficial).

8. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

9. En función del análisis de riesgos del banco de sus actividades de transferencias de fondos, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de actividades de transferencias de fondos de riesgo más alto, que pueden incluir lo siguiente:

   - Transferencias de fondos adquiridas con dinero en efectivo.

- Transacciones en las que el banco actúe como intermediario, como los pagos de cobertura.
- Transacciones en las que el banco remite o recibe transferencias de fondos de instituciones financieras extranjeras, particularmente desde o hacia jurisdicciones con leyes de secreto y privacidad estrictas, o aquellas identificadas como de riesgo más alto.
- Transacciones PUPID.

10. De la muestra seleccionada, analice las transferencias de fondos para determinar si las cantidades, la frecuencia y las jurisdicciones de origen o destino son coherentes con el tipo de negocio u ocupación del cliente.
11. Además, para las transferencias de fondos procesadas con los formatos de mensaje MT 202 y MT 202 COV, revise la muestra de mensajes para determinar si el banco ha utilizado los formatos de mensaje correctos y ha incluido toda la información del remitente y el beneficiario (por ejemplo, no falta información ni se incluyó información sin sentido).
12. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de transferencias de fondos.

Transacciones de Compensación Automatizada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la compensación automatizada (ACH) y las transacciones ACH internacionales (IAT), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

El uso de ACH ha aumentado notablemente en los últimos años debido al gran volumen de conversiones electrónicas de cheques[184] y débitos únicos en ACH, lo que refleja el bajo costo del procesamiento en ACH respecto al procesamiento de cheques.[185] Las transacciones de conversión de cheques, como los débitos únicos en ACH, generalmente involucran transacciones de particulares de poco valor en dólares para la adquisición de bienes y servicios o el pago de facturas de consumidores. ACH se utiliza principalmente para los pagos nacionales, pero el sistema FedGlobal[186] de los Bancos de la Reserva Federal actualmente admite los pagos transnacionales a muchos países del mundo.

En Septiembre de 2006, la Oficina del Interventor Monetario expidió una guía con el título *Automated Clearinghouse Activities — Risk Management Guidance* (Actividades de compensación automatizada: guía sobre gestión de riesgos). El documento proporciona una guía para gestionar los riesgos de la actividad de ACH. Los bancos pueden estar expuestos a una variedad de riesgos cuando originan, reciben o procesan transacciones de ACH o subcontratan un servicio externo para que realice estas actividades.[187]

Sistema de pagos ACH

Tradicionalmente, el sistema ACH se ha utilizado para el depósito directo de nómina y pagos de beneficios gubernamentales, y para el pago directo de hipotecas y préstamos. Como se indicó anteriormente, ACH se está expandiendo hasta incluir los débitos únicos

[184] En el proceso de conversión electrónica de cheques, los intermediarios que reciben un cheque para pago no cobran el cheque a través del sistema de cobro de cheques, ya sea electrónicamente o en papel. En cambio, los intermediarios utilizan la información del cheque para iniciar un tipo transferencia de fondos electrónica conocida como débito ACH de la cuenta del individuo que libra el cheque. El cheque se utiliza para obtener el número ABA del banco, número de cuenta, número de serie del cheque y suma en dólares de la transacción, pero el cheque en sí mismo no se envía a través del sistema de cobro de cheques en ninguna forma como instrumento de pago. Los intermediarios utilizan la conversión electrónica de cheques porque puede resultar una forma más eficaz de obtener los pagos que cobrando el cheque.

[185] Consulte www.nacha.org.

[186] Los Bancos de la Reserva Federal operan el FedACH, una institución de compensación central para transmitir y recibir pagos ACH, y FedGlobal, que envía pagos de créditos ACH transnacionales a más de 35 países del mundo y pagos de débito solamente a Canadá.

[187] Consulte el boletín de la OCC 2006-39 del 1.º de Septiembre de 2006) en www.occ.gov/ftp/bulletin/2006-39.pdf.

y la conversión de cheques. Las transacciones de ACH constituyen instrucciones de pago para acreditar o debitar de una cuenta de depósito. Los ejemplos de transacciones de pago con crédito incluyen los depósitos directos de nómina, Seguro Social, dividendos y pagos de intereses. Los ejemplos de transacciones con débito incluyen los pagos de hipoteca, préstamos, primas de seguro y una variedad de pagos de particulares iniciados a través de intermediarios (en inglés, *merchants*) o comercios.

Generalmente, una transacción de ACH es una transferencia de fondos electrónica procesada por lotes y con fecha efectiva entre un banco remitente y uno receptor. A una transacción de crédito ACH la origina el titular de cuenta que envía los fondos (pagador); en cambio, a una transacción de débito ACH la origina el titular de cuenta que recibe los fondos (beneficiario). Dentro del sistema ACH, estos participantes y usuarios se conocen con los siguientes términos:

- **Remitente.** Una organización o persona que inicia una transacción de ACH en una cuenta como un débito o un crédito.

- **Institución Financiera de Depósito de Origen (ODFI).** La institución financiera de depósito del remitente que envía la transacción de ACH a la red ACH nacional a través de un operador ACH.

- **Operador ACH.** Un operador ACH procesa todas las transacciones de ACH que fluyen entre las diferentes instituciones financieras de depósito. Un operador ACH sirve de institución de compensación central que recibe entradas de las ODFI y las distribuye a la Institución Financiera de Depósito Receptora correspondiente. Actualmente existen dos operadores ACH: Red de pago electrónico (EPN) y FedACH.

- **Institución Financiera de Depósito Receptora (RDFI).** La institución de depósito del Receptor que recibe la transacción de ACH de los operadores ACH y fondos de crédito o débito de las cuentas de los receptores.

- **Receptor.** Una organización o persona que autoriza al remitente a iniciar una transacción de ACH, ya sea como débito o crédito a una cuenta.

- **Operador de puerta de enlace (GO).** Una institución financiera, un operador ACH o una ODFI que actúa como un punto de entrada o de salida hacia o desde los Estados Unidos. Como operador de puerta de enlace, no se requiere una declaración formal de estado. Los operadores ACH y las ODFI que actúan como operadores de puerta de enlace tienen garantías y obligaciones específicas relacionadas con determinadas entradas internacionales. Una institución financiera que actúa como un operador de puerta de enlace generalmente puede procesar transacciones de débito y crédito de entrada y de salida. Los operadores ACH que actúan como operadores de puerta de enlace pueden procesar asientos de crédito y débito de salida, pero pueden limitar los asientos de entrada a asientos de crédito solamente y contraasientos.

Pagos ACH internacionales

NACHA: La Asociación de Pagos Electrónicos estableció formatos y normas operativas sobre las transacciones ACH internacionales (IAT) que entraron en vigencia el 18 de Septiembre de 2009.[188] IAT es un nuevo código de clase de entrada estándar para los pagos ACH que habilita a las instituciones financieras a identificar y supervisar los pagos ACH internacionales, y a realizar una revisión conforme a la OFAC. Las normas requieren que los operadores de puerta de enlace clasifiquen los pagos que son transmitidos a una agencia financiera[189] fuera de la jurisdicción territorial de los Estados Unidos, o bien que son recibidos desde la agencia, como IAT. La clasificación dependerá de la ubicación de la agencia financiera que administra la transacción de pago (movimiento de fondos) y no de la ubicación de cualquier otra parte de la transacción (por ejemplo, el remitente o el receptor).

De conformidad con las normas operativas de la NACHA, todas las instituciones financieras estadounidenses que participan en la red ACH deben poder utilizar el formato IAT.

Definición de IAT

Una IAT es una entrada ACH que es parte de una transacción de pago que involucra una oficina de una agencia financiera que no está ubicada en la jurisdicción territorial de los Estados Unidos. Una oficina de una agencia financiera está involucrada en una transacción de pago si se cumplen una o más de las siguientes condiciones:

- Tiene una cuenta que se acredita o debita como parte de la transacción de pago.
- Recibe fondos directamente de una persona o realiza pagos directamente a una persona como parte de una transacción de pago.
- Sirve de intermediaria en la liquidación de cualquier parte de una transacción de pago.

Términos relacionados con IAT

Un “asiento de entrada” se origina en otro país y se transmite a los Estados Unidos. Por ejemplo, un asiento de entrada puede ser la obtención de fondos para la nómina de una empresa. Cada IAT subsiguiente que se utilice para el depósito directo sería un asiento de IAT de entrada.

Un “asiento de salida” se origina en los Estados Unidos y se transmite a otro país. Por ejemplo, los pagos de jubilación de IAT de una ODFI estadounidense a una RDFI

[188] Si desea información adicional sobre las IAT, consulte www.nacha.org/c/IATIndustryInformation.cfm.

[189] “Agencia financiera” es una entidad que, según la ley aplicable, tiene autorización para aceptar depósitos o está en el negocio de realizar giros postales o transferencias de fondos.

estadounidense en la que los fondos luego se transfieren a una cuenta en otro país serían asientos de IAT de salida.

Guía de transacción de pago

Una transacción de pago es:

- la instrucción de un remitente a un banco de pagar, o de obtener el pago de, o de que otro banco pague u obtenga el pago de, una suma de dinero fija o determinada que se pagará a un receptor, o que se obtendrá de este; y
- todos y cada una de las liquidaciones, asientos contables o desembolsos que sean necesarios o adecuados para llevar a cabo la instrucción.

Identificación de las partes de IAT

Las normas operativas de la NACHA definen nuevas partes como parte de un asiento de IAT:

- Banco corresponsal extranjero: Una institución financiera de depósito participante (DFI) que retiene depósitos que son propiedad de otras instituciones financieras, y que proporciona pagos y otros servicios a dichas instituciones.
- Operador de puerta de enlace extranjera (FGO): Un operador de puerta de enlace que actúa como un punto de entrada o de salida desde un país extranjero.

Información adicional

El nuevo formato de IAT aumenta la cantidad de información del remitente y el beneficiario a la que los bancos tendrán acceso. Dicha información puede ser de utilidad en sus esfuerzos de supervisión, de prevención de lavado de dinero y OFAC.[190] Algunos ejemplos de la información que actualmente está a disposición de los bancos con el nuevo formato de IAT incluyen:

- Nombre y dirección del remitente.
- Nombre y dirección del receptor.
- Números de cuenta del remitente y el receptor.
- Nombre de la ODFI (IAT de entrada, DFI extranjera), número de identificación y código de país de la sucursal.

---

[190] Por conveniencia, esta información a menudo se denomina información "*Travel Rule*", pero por cuestiones técnicas las reglas de transmisión y gestión de registros de transferencias de fondos de 31 CFR 103.33(g) no se aplican a las transacciones ACH, y las reglas operativas de NACHA no han cambiado.

- Nombre de la RDFI (IAT de salida, DFI extranjera), número de identificación y código de país de la sucursal.
- Código de país.
- Código de divisa.
- Indicador de cambio de moneda extranjera.

Consulte www.nacha.org para obtener más información sobre los datos adicionales a disposición de los bancos con el nuevo formato de IAT.

Prestadores de servicios externos

Un prestador de servicios externo (TPSP) es una entidad distinta a un remitente, ODFI o RDFI que lleva a cabo cualquier función en nombre del remitente, la ODFI o la RDFI con respecto al procesamiento de entradas ACH.[191] Las normas operativas de la NACHA definen los TPSP y los subconjuntos relevantes de TPSP que incluyen "remitentes externos" y "puntos de envío".[192] Las funciones de estos TPSP pueden incluir, entre otras, la creación de archivos ACH en nombre del remitente o la ODFI, o actuando como punto de envío de una ODFI (o punto de recepción en nombre de una RDFI).

Factores de riesgo

El sistema ACH fue diseñado para transferir un gran volumen de transacciones de poco valor en dólares, que plantean riesgos BSA/AML menores. No obstante, la capacidad de enviar transacciones internacionales y de mayor valor en dólares a través de ACH puede exponer a los bancos a mayores riesgos BSA/AML. Los bancos sin un sistema de supervisión BSA/AML sólido pueden estar expuestos a riesgos adicionales particularmente cuando las cuentas se abren en Internet sin contacto directo.

Las transacciones ACH que se originan a través de TPSP (es decir, cuando el remitente no es un cliente directo de la ODFI) pueden incrementar los riesgos BSA/AML, dificultando por lo tanto la tarea de la ODFI de evaluar los riesgos y controlar las transacciones del remitente para verificar el cumplimiento con las normas BSA/AML.[193]

---

[191] Un prestador de servicios externo es un término genérico que abarca a cualquier negocio que preste servicios a un banco. Un procesador de pagos externo es un tipo específico de prestador de servicios que procesa los pagos como cheques, archivos ACH, o archivos o mensajes de tarjetas de crédito y débito. Consulte la sección del esquema general ampliado, "Procesadores de pagos externos", en las páginas 265 a 268, como guía.

[192] Cuando los TPSP independientes celebran un contrato con organizaciones de ventas independientes u otros procesadores de pagos externos, puede haber dos o más niveles entre la ODFI y el Remitente.

[193] La política de colocación de un banco debe definir qué información debe contener cada aplicación. La exhaustividad del control de la aplicación de un remitente debe coincidir con el nivel de riesgo planteado por él. La política de colocación debe exigir una verificación de antecedentes de cada remitente para respaldar la validez del negocio.

Los riesgos se incrementan cuando ni el TPSP ni el ODFI aplican debida diligencia a las compañías para las que están originando pagos.

Ciertas transacciones ACH, como las originadas a través de Internet o por teléfono, pueden ser susceptibles a la manipulación y el uso fraudulento. Ciertas prácticas asociadas con la manera en que la industria bancaria procesa las transacciones ACH pueden exponer a los bancos a riesgos BSA/AML. Estas prácticas incluyen:

- Una ODFI que autoriza a un TPSP a enviar archivos ACH directamente a un Operador ACH, esencialmente eludiendo la ODFI.
- Las ODFI y RDFI que dependen una de la otra para aplicar la debida diligencia adecuada a sus clientes.
- El procesamiento por lotes que permite ocultar la identidad de los remitentes.
- La imposibilidad de compartir información acerca de los remitentes y los receptores inhibe la capacidad de un banco para analizar y gestionar adecuadamente el riesgo asociado con las operaciones de procesamiento de ACH y cuentas corresponsales, supervisar las actividades sospechosas y corroborar el cumplimiento con la OFAC.

Mitigación del riesgo

La BSA exige a los bancos que dispongan de programas de cumplimiento BSA/AML y de políticas, procedimientos y procesos adecuados para supervisar e identificar actividades poco habituales, incluidas las transacciones ACH. La obtención de CDD en todas las operaciones es importante para mitigar el riesgo BSA/AML de las transacciones ACH. Debido al carácter de las transacciones ACH y la dependencia mutua de las ODFI y RDFI para realizar los controles OFAC y obtener otra información de debida diligencia necesaria, es esencial que todas las partes cuenten con un programa de CDD firme para los clientes ACH habituales. En las relaciones con TPSP, la CDD de los TPSP se puede complementar con debida diligencia de los mandantes asociados con el TPSP y, según sea necesario, de los remitentes. Las políticas, los procedimientos y los procesos de CDD adecuados son fundamentales para detectar un patrón de actividades sospechosas o poco habituales debido a que las transacciones ACH individuales generalmente no se controlan. Es igualmente importante contar con un sistema de informe y supervisión de actividades sospechosas eficaz en función del riesgo. En los casos en que un banco dependa en exceso del TPSP, es posible que el banco desee controlar el programa de informe y supervisión de actividades sospechosas del TPSP, ya sea a través de una inspección independiente o por su cuenta. La ODFI puede establecer un acuerdo con el TPSP, que defina pautas generales de TPSP, como el cumplimiento con las exigencias operativas y responsabilidades ACH, y otros reglamentos federales y estatales vigentes. Es posible que los bancos tengan que considerar la implementación de controles que restrinjan o nieguen los servicios ACH a remitentes y receptores potenciales que participen en prácticas comerciales cuestionables o engañosas.

Las transacciones ACH se pueden utilizar en las fases de transformación e integración del lavado de dinero. La detección de actividad poco habitual en las fases de transformación

e integración puede resultar una tarea dificultosa, ya que se puede utilizar ACH para legitimar las transacciones frecuentes y periódicas. Los bancos deben tener en cuenta las fases de transformación e integración del lavado de dinero cuando evalúen o analicen los riesgos de las transacciones ACH de un cliente en particular.

La ODFI debe estar al tanto de la actividad de las IAT y debe evaluarla usando un enfoque basado en el riesgo para asegurar la identificación y la supervisión de cualquier actividad sospechosa. La ODFI, si participa frecuentemente en las IAT, puede desarrollar un proceso separado para controlar las IAT que minimice la interrupción del procesamiento, la conciliación y la liquidación ACH; dicho proceso se puede automatizar.

Las políticas, los procedimientos y los procesos relacionados con ACH del banco deben contemplar el posible riesgo más alto inherente en las IAT. El banco debe considerar sus funciones y sus responsabilidades actuales y potenciales al desarrollar los controles internos para supervisar y mitigar el riesgo asociado con las IAT y para cumplir con las exigencias de gestión de registros de actividades sospechosas del banco.

En el procesamiento de las IAT, el banco debe considerar lo siguiente:

- El volumen y los tipos de transacciones y clientes.
- Las relaciones asociadas con los procesadores de pagos externos.
- Las responsabilidades, las obligaciones y los riesgos de convertirse en un GO.
- Las normas y las prácticas de CIP, CDD y EDD.
- El informe y la supervisión de actividades sospechosas.
- Los MIS adecuados, incluida la posible necesidad de realizar actualizaciones y cambios en los sistemas.
- Los procedimientos de procesamiento (por ejemplo, la identificación y la gestión de las IAT, la resolución de positivos de OFAC, y la gestión de los mensajes rechazados y que no cumplen con lo estipulado).
- Los programas de capacitación para el personal adecuado del banco (por ejemplo, el personal de ACH, operaciones, auditorías de cumplimiento, atención al cliente, etc.).
- Los acuerdos legales, incluyendo aquellos con clientes, procesadores externos y proveedores, y si dichos acuerdos deben ser actualizados o modificados.

Evaluación de la OFAC

Todas las partes involucradas en una transacción ACH están sujetas a las exigencias de la OFAC. (Consulte la sección del esquema general principal, “Oficina de control de activos extranjeros”, en las páginas 165 a 175, como guía). La OFAC ha aclarado la

aplicación de sus normas a las transacciones ACH nacionales y transnacionales, y proporcionó una guía más detallada sobre transacciones ACH internacionales.[194]

Con respecto a las transacciones ACH nacionales, la ODFI es responsable de verificar que el Remitente no sea una parte bloqueada y de esforzarse de buena fe por confirmar que éste no esté transmitiendo fondos bloqueados. Del mismo modo, la RDFI es responsable de verificar que el Receptor no sea una parte bloqueada. De este modo, la ODFI y la RDFI dependen mutuamente la una de la otra para cumplir con los reglamentos de la OFAC.

Si una ODFI recibe transacciones ACH nacionales que su cliente ya ha procesado por lotes, la ODFI no es responsable de anular este procesamiento por lotes para asegurarse de que ninguna transacción viole los reglamentos de la OFAC. Si una ODFI anula el procesamiento por lotes de un archivo recibido del Remitente para procesar transacciones *on-us*, tal ODFI es responsable de que las transacciones *on-us* cumplan con la OFAC, debido a que en este caso estará actuando como la ODFI y la RDFI en dichas transacciones. Las ODFI, actuando en esta calidad, deben conocer a sus clientes con anterioridad a los efectos de la OFAC y otras exigencias normativas. En relación con las transacciones residuales del archivo no procesadas por lotes que sean *on-us*, y a otras situaciones en las que los bancos manejen registros de ACH no procesados por lotes por motivos que no sean para desglosar las transacciones *on-us*, los bancos deben determinar el nivel de riesgo OFAC y desarrollar políticas, procedimientos y procesos adecuados para tratar los riesgos asociados. Dichas políticas atenuantes pueden implicar la revisión de cada registro de ACH no procesado por lotes. Del mismo modo, los bancos que entablan relaciones con prestadores de servicios externos deben analizar el carácter de dichas relaciones y sus transacciones ACH relacionadas para confirmar el nivel de riesgo según la OFAC del banco y para desarrollar políticas, procedimientos y procesos para mitigar ese riesgo.

Con respecto a las evaluaciones transnacionales, existen obligaciones similares aunque más estrictas de la OFAC para las IAT. En el caso de las IAT de entrada, e independientemente de si se establece la bandera de la OFAC en la IAT, una RDFI es responsable del cumplimiento con las exigencias de la OFAC Sin embargo, en el caso de las transacciones IAT de salida, la ODFI no puede depender de la evaluación de la OFAC por parte de una RDFI fuera de los Estados Unidos. En tales situaciones, la ODFI debe ejercer diligencia intensificada para garantizar que no se procesen transacciones ilegales.

La debida diligencia para una IAT de entrada o de salida puede incluir la evaluación de las partes para una transacción, así como la revisión de los detalles de la información del campo de pago de una indicación de violación a una sanción, la investigación de los positivos resultantes, en caso que existan, y, finalmente, el bloqueo o rechazo de la transacción, según corresponda. Consulte la sección del esquema general principal, “Oficina de control de activos extranjeros”, en las páginas 165 a 175, como guía.

---

[194] Consulte la nota explicativa 041214-FACRL-GN-02 en www.treas.gov/offices/enforcement/ofac/rulings/. Las normas NACHA especifican aún más este cumplimiento (consulte la página 8 de la sección sobre búsqueda rápida de *2006 NACHA Operating Rules* [Normas operativas NACHA 2006]).

En una guía emitida el 10 de marzo de 2009, la OFAC autorizó a instituciones en los Estados Unidos, cuando actúen como una ODFI o un GO para débitos de IAT de entrada, a rechazar transacciones que parezcan involucrar intereses de propiedad o propiedad bloqueable.[195] La guía establecía además que en la medida que una ODFI o un GO evalúen los débitos de IAT de entrada para determinar si existen posibles violaciones a la OFAC antes de la ejecución y en el transcurso de dicha evaluación descubren una potencial violación a la OFAC, la transacción sospechosa se deberá eliminar del lote para realizar una investigación más profunda. Si la ODFI o el GO determinan que la transacción no parece violar los reglamentos de la OFAC, deben negarse a procesar la transferencia. El procedimiento se aplica a las transacciones que normalmente serían bloqueadas así como para las transacciones que normalmente serían rechazadas por propósitos de la OFAC en función de la información de los pagos.

Más información sobre los tipos de sistemas de pago al por menor (sistemas de pago ACH) está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[196]

---

[195] Consulte www.frbservices.org/files/eventseducation/pdf/iat/031809_ofac_update.pdf.

[196] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Procedimientos de Inspección

Transacciones de compensación automatizada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la compensación automatizada (ACH) y las transacciones ACH internacionales (IAT), y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las transacciones ACH, incluidas las IAT. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de transacciones ACH del banco, incluidas las IAT, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz los clientes de riesgo más alto que efectúan transacciones ACH, incluidas las IAT.

3. Evalúe los riesgos del banco relacionados con las transacciones ACH, incluidas las IAT, analizando la frecuencia y el volumen en dólares y los tipos de transacciones ACH en relación con el tamaño, la ubicación y el carácter de las relaciones asociadas con las cuentas de los clientes del banco, y la ubicación de la fuente y el destino de las IAT con relación a la ubicación del banco.

4. Determine si el sistema del banco para supervisar a los clientes, incluidos los prestadores de servicios externos (TPSP), que efectúan transacciones ACH y IAT y detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de control interno incluyen:

   - La identificación de clientes con IAT o transacciones ACH de grandes volúmenes y frecuentes.

   - La supervisión de la actividad de detalles de ACH cuando las transacciones procesadas por lotes se separan para otros fines (por ejemplo, el procesamiento de errores).

   - Según corresponda, la identificación y la aplicación de la debida diligencia intensificada a clientes de mayor riesgo que originan o reciben IAT, en especial cuando una parte de la transacción se encuentra en una ubicación geográfica de mayor riesgo.

   - La utilización de métodos para hacer seguimiento, revisar e investigar los retornos no autorizados o las quejas de los clientes sobre posibles transacciones ACH duplicadas o fraudulentas, incluyendo IAT.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de los clientes con transacciones ACH, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de clientes de riesgo más alto, incluidos los TPSP, con transacciones ACH o IAT, que puede incluir lo siguiente:

   - Clientes que inician transacciones ACH, incluidas las IAT, que se originan en Internet o por teléfono, particularmente desde una cuenta que se abre en Internet o por teléfono sin interacción personal directa.
   - Clientes cuyos tipos de negocios u ocupaciones no requieren el volumen ni el carácter de la actividad de ACH o IAT.
   - Clientes que hayan participado en el origen o la recepción de IAT o transacciones ACH duplicadas o fraudulentas.
   - Clientes remitentes (clientes de clientes) que generan un alto porcentaje o alto volumen de retorno sobre la inversión inválidos, retorno sobre la inversión no autorizado o u otras transacciones no autorizadas.

7. De la muestra seleccionada, analice las transacciones ACH, incluidas las IAT, para determinar si las cantidades, la frecuencia y las jurisdicciones de origen y destino son coherentes con el tipo de negocio u ocupación del cliente. Un control de la documentación de apertura de la cuenta, incluida la documentación del CIP, puede ser necesario para tomar estas determinaciones. Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a las IAT y las transacciones ACH.

Efectivo Electrónico: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el efectivo electrónico (e-cash), y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

El efectivo electrónico (dinero electrónico) es una representación digital del dinero. El efectivo electrónico adopta diversas formas, entre ellos, medios informáticos, medios de telefonía móvil y tarjetas prepagadas. El efectivo electrónico se almacena en un repositorio en línea y el acceso a este se obtiene vía módem por medio de los discos rígidos de las computadoras personales. El acceso al efectivo electrónico basado en la telefonía móvil se obtiene a través del teléfono móvil de una persona. Las tarjetas prepagadas, descritas más detalladamente a continuación, se utilizan para obtener acceso a fondos retenidos por bancos emisores en cuentas agrupadas.

En el caso del efectivo electrónico por medio de computadora, el valor monetario se deduce electrónicamente de la cuenta bancaria cuando se realiza una compra o se transfieren fondos a otra persona. Hay más información sobre los tipos de productos de efectivo electrónico en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC.[197]

Factores de riesgo

Las transacciones que utilizan efectivo electrónico pueden plantear al banco los siguientes riesgos particulares:

- Los fondos se pueden transferir desde o hacia un tercero desconocido.
- Los clientes pueden evitar las restricciones impuestas en las fronteras ya que las transacciones tienen la capacidad de hacerse móviles y pueden no estar sujetas a restricciones jurisdiccionales.
- Las transacciones pueden ser instantáneas.
- La actividad específica del titular de la tarjeta puede ser difícil de determinar controlando la actividad a través de una cuenta agrupada.
- El cliente puede percibir que las transacciones son menos transparentes.

Mitigación del riesgo

Los bancos deben establecer una supervisión, identificación y presentación de informes BSA/AML de actividades sospechosas y poco habituales que ocurran a través de efectivo

[197] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

electrónico. Los MIS útiles para detectar las actividades poco habituales en cuentas de riesgo más alto incluyen los informes de actividad de cajeros automáticos (enfocándose en las transacciones extranjeras), informes de transferencias de fondos, informes de actividad de cuentas nuevas, informes de cambio de dirección de Internet, informes de direcciones de Protocolo de Internet (IP, por sus siglas en inglés) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, direcciones, números telefónicos, direcciones de correo electrónico y números de identificación fiscal comunes). Además, el banco puede implementar otros controles, como el establecimiento de límites en dólares por transacción o cuenta que requieran intervención manual para superar el límite preestablecido.

Tarjetas prepagadas/Tarjetas de valor acumulado

De acuerdo con la práctica de la industria, en este documento se utiliza principalmente el término “tarjeta prepagadas”. Si bien en general algunas fuentes utilizan el término “tarjeta de valor acumulado”, con mayor frecuencia se refiere a las tarjetas en las que el valor monetario está físicamente almacenado en la tarjeta. Por lo general, el término “tarjeta prepagadas” se refiere a un dispositivo de acceso vinculado a fondos retenidos en una cuenta agrupada, que es el tipo de producto que más frecuentemente ofrecen las organizaciones bancarias estadounidenses. Las tarjetas prepagadas pueden cubrir una variedad de productos, funcionalidades y tecnologías, y funcionan dentro de sistemas “abiertos”
o “cerrados”. Las tarjetas prepagadas de sistemas abiertos se pueden utilizar para realizar compras en cualquier intermediario o para obtener acceso a efectivo en cualquier cajero automático (ATM) conectado a la red de pago global afiliada. Algunos ejemplos de tarjetas de sistemas abiertos son las tarjetas de nómina y las tarjetas de regalo que se pueden utilizar en cualquier lugar donde se pueda utilizar una tarjeta de crédito. Algunas tarjetas prepagadas se pueden recargar, lo que permite que el titular de la tarjeta agregue valor. En general, las tarjetas de sistemas cerrados sólo se pueden utilizar para adquirir bienes o servicios del intermediario que expide la tarjeta o de un grupo selecto de intermediarios o prestadores de servicios que participan en una red específica. Algunos ejemplos de tarjetas de sistemas cerrados incluyen las tarjetas de regalo de tiendas minoristas específicas de los intermediarios, las tarjetas de los centros comerciales y las tarjetas de transporte público

Algunos programas de tarjetas prepagadas pueden combinar varias características, como una a tarjeta de gastos flexible que se pueden utilizar para adquirir determinados servicios de salud y productos de una amplia gama de intermediarios. A menudo estos programas se denominan tarjetas “híbridas”.

Las tarjetas prepaga proporcionan una forma compacta y trasladable de mantener y obtener acceso a fondos. Además, ofrecen a las personas que no tienen una cuenta bancaria una alternativa de acceso a efectivo y giros postales. Como un método alternativo de transferencias de fondos transnacionales, los programas de tarjetas prepaga pueden emitir varias tarjetas por cuenta, de modo que otras personas en otro país puedan obtener acceso a los fondos cargados por el titular de la tarjeta mediante extracciones de ATM o compras a intermediarios.

Muchos bancos ofrecen programas de tarjetas prepagadas como bancos emisores. La mayoría de las redes de pago requieren que sus tarjetas prepagadas de marca sean emitidas por un banco que sea miembro de dicha red de pago. Además de emitir tarjetas prepagadas, los bancos pueden participar en otros aspectos de un programa de tarjetas, como la comercialización y la distribución de tarjetas emitidas por otra institución financiera.

Con frecuencia, los bancos dependen de diversos terceros para lograr el diseño, la implementación y el mantenimiento de sus programas de tarjetas prepagadas. Estos terceros pueden incluir administradores de programas, distribuidores, vendedores, intermediarios y procesadores. Conforme a los requisitos de la red de pago, el banco emisor puede tener debida diligencia y otras responsabilidades relacionadas con estos terceros.

Acuerdos contractuales

Cada relación que un banco estadounidense mantenga con terceros o instituciones financieras como parte de un programa de tarjetas prepagadas debe regirse por un acuerdo o contrato que especifique las responsabilidades de cada una de las partes y otros detalles de la relación, como los productos y los servicios provistos. El acuerdo o contrato también debe considerar las exigencias de cumplimiento de OFAC y BSA/AML de cada parte, el tipo de clientela, los procedimientos de debida diligencia y las obligaciones de la red de pago. El banco emisor tiene la responsabilidad final con respecto al cumplimiento BSA/AML, ya sea que el acuerdo contractual se haya establecido o no.

Factores de riesgo

Si no hay controles eficaces implementados, a través de los programas de tarjetas prepagadas se pueden llevar a cabo lavado de dinero, financiamiento del terrorismo y otras actividades delictivas. Mediante investigaciones a cargo de las autoridades de aplicación de la ley, se ha descubierto que algunos titulares de tarjetas prepagadas utilizaban identificaciones falsas y financiaban los depósitos iniciales con tarjetas de crédito robadas o compraban varias tarjetas bajo sobrenombres. En la etapa de colocación del lavado de dinero, dado que muchos bancos nacionales y extraterritoriales ofrecen acceso a efectivo internacionalmente vía ATM, los delincuentes pueden cargar efectivo de fuentes ilícitas en tarjetas prepagadas a través de puntos de carga no regulados y enviar las tarjetas a sus cómplices dentro o fuera del país. Las investigaciones han revelado que las tarjetas prepagadas de sistemas abiertos y cerrados han sido utilizadas junto con, o como un reemplazo de, el contrabando de efectivo en grandes cantidades. Los terceros involucrados en los programas de tarjetas prepagadas pueden o no estar sujetos a exigencias normativas, control y supervisión. Además, estas exigencias pueden variar según las partes.

Los programas de tarjetas prepagadas son extremadamente diversos en la gama de productos y servicios provistos y en las bases de clientes que cubren. Al evaluar el perfil de riesgo de un programa de tarjetas prepagadas, los bancos deben considerar las características y las funcionalidades específicas del programa. No existe un único indicados que sea necesariamente determinante de un riesgo BSA/AML más alto o más bajo. El riesgo de lavado de dinero potencialmente más alto asociado con las tarjetas

prepagadas deriva del anonimato del titular de la tarjeta, la información falsa sobre el titular de la tarjeta, el acceso a efectivo que brinda la tarjeta (en especial internacionalmente)
y el volumen de fondos que pueden tramitarse con la tarjeta. Otros factores de riesgo incluyen el tipo y la frecuencia de las transacciones y las cargas de la tarjeta, la ubicación geográfica de la actividad de la tarjeta, las relaciones con terceros en el programa de la tarjeta, los límites de valor de la tarjeta, los canales de distribución y la naturaleza de las fuentes de financiación.

Mitigación del riesgo

Los bancos que ofrecen tarjetas prepagadas o que de alguna otra forma participan en programas de tarjetas prepagadas deben tener políticas, procedimientos y procesos suficientes para gestionar los riesgos BSA/AML relacionados. La guía que ofrece la Network Branded Prepaid Card Association (Asociación de la red de tarjetas prepagadas de marca) es un recurso adicional para los bancos que prestan servicios de tarjetas prepagadas.[198] La debida diligencia de los clientes es importante para mitigar el riesgo BSA/AML de los programas de tarjetas prepagadas. El programa CDD de un banco debe proporcionar un análisis de riesgos de todos los terceros involucrados en el programa de tarjetas prepagadas que considere todos los factores relevantes y que incluya, según corresponda:

- La identidad y la ubicación de todos los terceros involucrados en el programa de tarjetas prepagadas, incluidos los subagentes.
- La documentación corporativa, las licencias y las referencias (incluidos los servicios de informe independiente) y, si corresponde, la documentación sobre los propietarios principales.
- La naturaleza de las empresas de los terceros, y los intermediarios y las bases de clientes cubiertos.
- La información recopilada para identificar y verificar la identidad del titular de la tarjeta.
- El tipo, el propósito y la actividad prevista del programa de tarjetas prepagadas.
- La naturaleza y la duración de la relación del banco con los terceros en el programa de las tarjetas.
- Las obligaciones según la OFAC y BSA/AML de los terceros.

---

[198] Consulte *Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs* (Prácticas recomendadas para el cumplimiento contra el lavado de dinero para los programas de tarjetas prepagadas basados en los Estados Unidos, del 28 de Febrero de 2008, en www.nbpca.com/docs/NBPCA-AML-Recommended-Practices-080220.pdf.

Como parte de su sistema de controles internos, los bancos deben establecer un medio para supervisar, identificar e informar las actividades sospechosas relacionadas con los programas de tarjetas prepagadas. Esta exigencia de gestión de registros se aplica a todas las transacciones que realiza el banco o que se realizan en o a través del banco, incluidas aquellas en un formulario adicional. Es posible que los bancos necesiten establecer protocolos para obtener periódicamente información de las transacciones con tarjeta por parte de procesadores y otros terceros. Los sistemas de supervisión deben tener la capacidad para identificar la actividad de las tarjetas en el extranjero, las compras de grandes cantidades realizadas por una persona y las compras múltiples realizadas por terceros relacionados. Además, los procedimientos deben incluir la supervisión de patrones de actividad poco habitual, como las cargas de tarjetas de crédito seguidas inmediatamente de extracciones del importe total desde otra ubicación.

Las características de las tarjetas pueden proporcionar una mitigación significativa de los riesgos BSA/AML inherentes a las transacciones y las relaciones de tarjetas prepagadas, y pueden incluir:

- Límites o prohibiciones de carga, acceso o reembolso de efectivo.
- Límites o prohibiciones respecto de los importes de las cargas y la cantidad de cargas/recargas en un plazo dado (velocidad de uso de los fondos).
- Controles sobre la cantidad de tarjetas adquiridas por un individuo.
- Umbrales en dólares máximos en las extracciones de ATM y en la cantidad de extracciones en un plazo dado (velocidad del uso de los fondos).
- Límites o prohibiciones respecto de determinado uso (por ejemplo, tipo de intermediario) y del uso geográfico, como fuera de los Estados Unidos.
- Límites con respecto a los valores de tarjetas agregados.

Procedimientos de Inspección

Efectivo electrónico

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con el efectivo electrónico (e-cash), incluidas las tarjetas prepagadas, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto al efectivo electrónico, incluidas las tarjetas prepagadas. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de efectivo electrónico del banco, incluidas las tarjetas prepagadas, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las transacciones de banca electrónica de riesgo más alto, incluidas las transacciones con tarjetas prepagadas.

3. Determine si el sistema del banco para supervisar las transacciones de banca electrónica, incluidas las transacciones con tarjetas prepagadas, y para detectar e informar actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de efectivo electrónico, incluidas las transacciones con tarjetas prepagadas, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las transacciones con efectivo electrónico. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluida la del CIP, la debida diligencia continua de los clientes y los antecedentes de transacciones.
   - Compare la actividad prevista con la actividad real.
   - Determine si la actividad es coherente con el tipo de negocio del cliente.
   - Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con efectivo electrónico.

Procesadores de Pagos Externos: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con sus relaciones con los procesadores de pagos externos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

Los procesadores de pagos externos o no bancarios (procesadores) son clientes de bancos que prestan servicios de procesamiento de pagos a intermediarios y otras entidades comerciales. Tradicionalmente, los procesadores eran contratados principalmente por vendedores minoristas que tenían ubicaciones físicas para procesar sus transacciones. Estas transacciones de intermediarios incluían principalmente pagos con tarjetas de crédito pero también abarcaban transacciones de ACH, cheques creados remotamente (RCC)[199] y transacciones con tarjetas de débito o prepagadas. Con la expansión de Internet, las fronteras de los minoristas se han eliminado. En la actualidad, los procesadores prestan servicios a una variedad de cuentas de intermediarios, incluidos los comercios en Internet y los minoristas convencionales, las empresas de viajes prepagos, los *telemarketers* y los servicios de apuestas por Internet.

Los procesadores de pagos externos con frecuencia utilizan sus cuentas bancarias comerciales para realizar el procesamiento de pago de sus clientes intermediarios. Por ejemplo, el procesador puede depositar en su cuenta los RCC emitidos a nombre de un cliente intermediario o actuar como un remitente externo de transacciones ACH. En cualquiera de los casos, el banco no tiene una relación directa con el intermediario. El aumento del uso de los RCC por parte de los clientes de los procesadores, en especial los *telemarketers*, también aumenta el riesgo de procesamiento de pagos fraudulentos a través de la cuenta bancaria del procesador. La Corporación Federal de Seguro de Depósitos y la Oficina del Interventor Monetario han publicado una guia con relación a los riesgos, incluyendo los riesgos BSA/AML, asociados con los procesadores bancarios externos.[200]

Factores de riesgo

Generalmente, los procesadores no están sujetos a exigencias normativas BSA/AML. Como resultado, algunos procesadores pueden ser vulnerables al lavado de dinero, el robo de identidad y las estratagemas de fraude, y las transacciones ilícitas o las transacciones prohibidas por la OFAC.

---

[199] Un cheque creado remotamente (algunas veces llamado "giro a la vista") es un cheque que no es creado por el banco pagador (con frecuencia creado por un beneficiario o su prestador de servicios), librado de la cuenta bancaria de un cliente. Con frecuencia, el cliente autoriza el cheque remotamente, por teléfono o en línea y, por lo tanto, no lleva su firma de puño y letra.

[200] *Guidance on Payment Processor Relationships* (Guía sobre las relaciones con procesadores de pagos), FDIC FIL-127-2008, del 7 de Noviembre de 2008, y *Risk Management Guidance: Payment Processors* (Guía de gestión de riegos: procesadores de pagos), Boletín 2008-12 de la OCC, del 24 de Abril de 2008.

Los riesgos BSA/AML del banco al manejar una cuenta del procesador son similares a los riesgos de otras actividades en las que el cliente del banco efectúa transacciones a través del banco en nombre de los clientes del cliente. Cuando el banco no puede identificar ni comprender el carácter y fuente de las transacciones procesadas a través de una cuenta, los riesgos a los que se expone el banco y la probabilidad de actividades sospechosas pueden aumentar. Si un banco no ha implementado un programa de aprobación de procesadores adecuado que vaya más allá de la gestión de riesgos del crédito, podría ser vulnerable al procesamiento de transacciones ilícitas o sancionadas por la OFAC.

Los bancos que tienen clientes de procesadores de pagos externos deben estar al tanto de la mayor probabilidad de riesgo de retornos no autorizados y el uso de servicios por parte de intermediarios de alto riesgo. Algunos intermediarios de alto riesgo utilizan a terceros de forma rutinaria para procesar sus transacciones por la dificultad que tienen para establecer una relación directa con un banco. Estas entidades pueden incluir ciertas compañías de solicitud de pedidos por vía telefónica o por correo, compañías de *telemarketing*, las operaciones de apuestas en línea, los prestamistas de día de pago en línea, las empresas instaladas en el exterior y las empresas de entretenimiento para adultos. Los procesadores de pagos tienen un mayor riesgo de lavado de dinero y fraude si no tienen un medio eficaz para verificar las identidades y las prácticas comerciales de los clientes intermediarios. Los riesgos aumentan cuando el procesador no lleva a cabo la debida diligencia con respecto a los intermediarios para los que están originando los pagos.

Mitigación del riesgo

Los bancos que ofrezcan servicios de cuentas a procesadores deben desarrollar y mantener políticas, procedimientos y procesos adecuados para abordar los riesgos relacionados con estas relaciones. Como mínimo, estas políticas deben legitimar las operaciones comerciales del procesador y analizar su nivel de riesgo. Un banco puede evaluar los riesgos asociados con los procesadores de pagos al considerar:

- La implementación de una política que requiera una verificación de antecedentes inicial del procesador (por ejemplo, mediante el sitio web de la Comisión Federal de Comercio, la Better Business Bureau, departamentos de incorporación estatal, investigaciones por Internet y otros procesos de investigación) y de los intermediarios subyacentes del procesador, en función del riesgo con el objeto de verificar su solvencia y las prácticas comerciales generales.

- La revision de los materiales promocionales del procesador, incluido su sitio web, para determinar la clientela objetivo. Un banco puede desarrollar políticas, procedimientos y procesos que limiten los tipos de entidades permisibles para procesar servicios. Estas entidades pueden incluir entidades de riesgo más alto, como las compañías extraterritoriales, las operaciones relacionadas con el servicio de apuestas en línea, los *telemarketers* y los prestamistas de día de pago en línea. Estas restricciones deben ser claramente comunicadas al procesador al momento de la apertura de la cuenta.

- La determinación de si el procesador revende sus servicios a un tercero que se pueda definir como "agente o proveedor de oportunidades de Organización de ventas independiente" (ISO) o acuerdos de "puerta de enlace".[201]

- El control de las políticas, los procedimientos y los procesos del procesador para determinar la aptitud de sus normas de debida diligencia para los nuevos intermediarios.

- La solicitud al procesador de identificar a sus principales clientes al proporcionar información como el nombre del intermediario, su actividad comercial principal y su ubicación geográfica.

- La verificación directa, a través del procesador, de que el intermediario dirige una empresa legítima al comparar la información de identificación del intermediario con las bases de datos de los registros públicos y las bases de datos de fraude y cheques bancarios.

- La revision de documentación corporativa, incluidos los servicios de informe independiente y, si es aplicable, documentación sobre los propietarios principales.

- Visita al centro de operaciones comerciales del procesador.

Los bancos que prestan servicios de cuentas a procesadores de pagos externos deben supervisar sus relaciones con el procesador para detectar cualquier cambio significativo en las estrategias comerciales de éste que pueda tener efecto sobre su perfil de riesgo. Los bancos deben volver a verificar y actualizar periódicamente los perfiles de los procesadores para garantizar que el análisis de riesgos sea adecuado.

Además de los procedimientos adecuados y eficaces de debida diligencia y de apertura de la cuenta para las cuentas de procesadores, la gerencia debe supervisar estas relaciones para detectar actividades sospechosas o poco habituales. Para supervisar de manera eficaz estas cuentas, el banco debe contar con una comprensión de la siguiente información del procesador:

- Base del intermediario.

- Actividades del intermediario.

- Cantidad promedio de volumen en dólares y cantidad de transacciones.

- Volumen de "lecturas magnéticas" frente a "ingreso de datos" de las transacciones con tarjetas de crédito.

---

[201] Los acuerdos de puerta de enlace son similares a un proveedor de servicios de Internet con mayor capacidad de almacenamiento que vende esta capacidad a un tercero, quien a su vez distribuye servicios informáticos a otras personas diversas desconocidas por el proveedor. El tercero tomará las decisiones sobre quién recibirá el servicio, aunque el proveedor será el que proporcione la capacidad de almacenamiento final. Por lo tanto, el proveedor carga con todos los riesgos y recibe una ganancia menor.

- Antecedentes de reintegro del cobro, incluido el porcentaje de retorno sobre la inversión de las transacciones con débito de ACH y los RCC.

- Quejas de los clientes que sugieran que los clientes intermediarios de un procesador de pagos están obteniendo indebidamente información de cuentas personales y la están usando para generar débitos en ACH o RCC no autorizados.

Con respecto a la supervisión de cuentas, un banco debe investigar minuciosamente los altos niveles de retorno. La decision de aceptar o no altos niveles de retorno no debe ser basada la garantía colateral u otro medio de seguridad proporcionada por el procesador al banco. Un banco debe implementar políticas, procedimientos y procesos adecuados que aborden los riesgos de cumplimiento y fraude. Los altos niveles de débitos en ACH o RCC devueltos por fondos insuficientes o usos no autorizados pueden ser un indicador de fraude o actividad sospechosa.

Procedimientos de Inspección

Procesadores de pagos externos

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con sus relaciones con los procesadores de pagos externos, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los procesadores de pagos externos (procesadores). Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de procesador del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los MIS y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones con los procesadores, particularmente aquellas que presenten un riesgo más alto de lavado de dinero.

3. Determine si el sistema de supervisión de las cuentas de los procesadores del banco para detectar e informar de actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de control de activos extranjeros", en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de procesador, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de los procesadores de riesgo más alto. De la muestra seleccionada:

   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones para determinar los resultados de la comparación de las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el carácter de la actividad indicada del procesador.
   - Evalúe los controles relacionados con la identificación de altos índices de retornos no autorizados y el proceso vigente para abordar los riesgos de cumplimiento y fraude.
   - Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las cuentas de los procesadores.

Compraventa de Instrumentos Monetarios: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los instrumentos monetarios, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales para la compraventa de instrumentos monetarios para proporcionar un análisis más minucioso de los riesgos de lavado de dinero asociados con esta actividad.*

Los instrumentos monetarios son productos proporcionados por bancos e incluyen cheques de caja, cheques de viajeros y giros postales. Generalmente, los instrumentos monetarios se compran para pagar transacciones personales o comerciales y, en el caso de los cheques de viajeros, como forma de valor acumulado para futuras compras.

Factores de riesgo

La compra o cambio de instrumentos monetarios en las fases de colocación y transformación del lavado de dinero puede ocultar la fuente de ingresos ilícitos. Como resultado, los bancos han sido objetivos importantes en las operaciones de lavado debido a que proporcionan y procesan instrumentos monetarios a través de depósitos. Por ejemplo, se sabe que tanto clientes como quienes no son clientes han comprado instrumentos monetarios en sumas por debajo del umbral de USD 3.000 para evitar tener que proporcionar la identificación adecuada. Posteriormente, los instrumentos monetarios se colocan en las cuentas de depósito para eludir el umbral de presentación de CTR.

Mitigación del riesgo

Los bancos que vendan instrumentos monetarios deben disponer de políticas, procedimientos y procesos adecuados para mitigar el riesgo. Las políticas deben definir:

- Las transacciones con instrumentos monetarios aceptables y no aceptables (por ejemplo, transacciones de individuos que no son clientes, instrumentos monetarios con beneficiarios en blanco, instrumentos monetarios sin firma, exigencias de identificación para transacciones fraccionadas o la compra de múltiples instrumentos monetarios numerados en secuencia para el mismo beneficiario).

- Procedimientos para el control y detección de actividades sospechosas o poco habituales, incluida la derivación de cualquier inquietud a la gerencia.

- Los criterios de cese de las relaciones o negación a realizar negocios con individuos que no son clientes que hayan estado involucrados ininterrumpida y flagrantemente en actividades sospechosas.

Procedimientos de Inspección

Compraventa de instrumentos monetarios

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con los instrumentos monetarios, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión e informe. Esta sección amplía la revisión principal de las exigencias normativas y legales para la compraventa de instrumentos monetarios para proporcionar un análisis más minucioso de los riesgos de lavado de dinero asociados con esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a la venta de instrumentos monetarios. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de instrumentos monetarios del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger de manera razonable al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir del volumen de ventas y la cantidad de ubicaciones en las que se venden instrumentos monetarios, determine si el banco gestiona de manera adecuada el riesgo asociado con las ventas de instrumentos monetarios.

3. Determine si el sistema de supervisión de los instrumentos monetarios del banco para detectar e informar de actividades sospechosas, es adecuado dados el volumen de ventas de instrumentos monetarios, el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco. Determine si los sistemas de supervisión e informe de actividades sospechosas (manuales o automatizados) incluyen un control de:

   - Las ventas de instrumentos monetarios numerados en secuencia del mismo comprador o compradores diferentes para el mismo beneficiario y en un mismo día.
   - Las ventas de instrumentos monetarios al mismo comprador o ventas de instrumentos monetarios a compradores diferentes a nombre del mismo emisor.
   - Las compras de instrumentos monetarios por parte de quienes no son clientes.
   - Los compradores, beneficiarios y domicilios comunes, compras numeradas en secuencia y símbolos poco habituales.[202]

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de control de activos extranjeros”, en las páginas 176 a 178, como guía.

[202] Se sabe que quienes lavan dinero identifican la propiedad o fuente de los fondos ilegales a través del uso de impresiones únicas y poco habituales.

Pruebas de transacciones

5. En función del análisis de riesgos del banco, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de transacciones con instrumentos monetarios tanto para clientes como para quienes no son clientes de:

   - Registros de ventas de instrumentos monetarios.
   - Copias de instrumentos monetarios compensados comprados en efectivo.

6. De la muestra seleccionada, analice la información de transacción para determinar si las sumas, la frecuencia de las compras y los beneficiarios involucrados son consistentes con la actividad prevista de los clientes o quienes no son clientes (por ejemplo, pago de servicios públicos o compras domésticas). Identifique cualquier actividad sospechosa o poco habitual.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con los instrumentos monetarios.

Depósitos Mediante Agentes: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con respecto a depósitos mediante agentes, y la capacidad de la gerencia para implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Para muchos bancos, el uso de depósitos mediante agentes es una fuente común de financiamiento. Los avances recientes en la tecnología permiten que los agentes proporcionen a los banqueros un mayor acceso a una gran variedad de inversionistas potenciales que no están relacionados con el banco. Los depósitos se pueden obtener en Internet, a través servicios de cotización de certificados de depósito o a través de otros métodos publicitarios.

Los agentes de depósitos proporcionan servicios intermediarios para bancos e inversionistas. Esta actividad se considera de alto riesgo debido a que cada agente de depósito opera bajo sus propias pautas para obtener depósitos. El nivel de supervisión regulatoria de los agentes de depósito varía, como también la aplicabilidad directa de las exigencias BSA/AML a estos. Sin embargo, el agente de depósito está sujeto a las exigencias de la OFAC independientemente de su nivel regulatorio. Por consiguiente, es posible que el agente de depósito no esté llevando a cabo debida diligencia de los clientes o una evaluación de la OFAC adecuadas. Para obtener más información, consulte la sección del esquema general principal "Oficina de Control de Activos Extranjeros," en las páginas 165 a 175, o los procedimientos de inspección de la sección principal "Programa de identificación de clientes", en las páginas 65 a 68.[203] El banco que acepte depósitos mediante agentes dependerá del agente de depósitos para llevar a cabo de manera suficiente los procedimientos de apertura de la cuenta exigidos y cumplir con las exigencias de BSA/AML aplicables.

Factores de riesgo

Los riesgos de lavado de dinero y financiamiento del terrorismo surgen debido a que el banco puede no tener conocimiento de los usufructuarios finales o del origen de los fondos. El agente de depósito puede representar a una variedad de clientes que puede plantear un riesgo más alto de lavado de dinero y financiamiento del terrorismo (por ejemplo, clientes no residentes o extraterritoriales, personalidades sujetas a exposición política [PEP] o bancos fantasmas extranjeros).

[203] A los efectos de la reglamentación del CIP, en el caso de los depósitos mediante agentes, el "cliente" será el agente que abre la cuenta. Un banco no necesitará examinar la cuenta del agente de depósito para determinar la identidad de cada cotitular de cuenta en particular, sólo necesitará verificar la identidad del titular de la cuenta designado.

Mitigación del riesgo

Los bancos que acepten las cuentas o fondos de agentes de depósito deben desarrollar políticas, procedimientos y procesos adecuados que establezcan procedimientos de CDD mínimos para todos los agentes de depósito que provean depósitos al banco. El nivel de debida diligencia que un banco lleve a cabo debe ser acorde a su conocimiento del agente de depósito y las prácticas comerciales y base de clientes conocidas del agente de depósito.

En un intento por ocuparse del riesgo inherente en ciertas relaciones asociadas con agentes de depósito, los bancos pueden contemplar la celebración de un contrato firmado que establezca los papeles y responsabilidades de cada parte y las restricciones de ciertos tipos de clientes (por ejemplo, clientes no residentes o extraterritoriales, PEP o bancos fantasmas extranjeros). Los bancos deben realizar debida diligencia suficiente a los agentes de depósitos, en especial a los no regulados, desconocidos, extranjeros o independientes. Para gestionar los riesgos BSA/AML asociados con depósitos mediante agentes, el banco debe:

- Determinar si el agente de depósito constituye una empresa legítima en todas las ubicaciones operativas donde opera.
- Controlar las estrategias comerciales del agente de depósito, incluidos los mercados de clientes objetivo (por ejemplo, clientes nacionales y extranjeros) y los métodos de persuasión de los clientes.
- Determinar si el agente de depósito está sujeto a supervisión regulatoria.
- Evaluar si las políticas, los procedimientos y los procesos BSA/AML y según la OFAC del agente de depósito son adecuados (por ejemplo, confirmar si el agente de depósito lleva a cabo CDD suficiente, incluidos procedimientos del CIP).
- Determinar si el agente de depósito evalúa a los clientes para detectar coincidencias con la lista de la OFAC.
- Evaluar la aptitud de las auditorías BSA/AML y según la OFAC del agente de depósito y asegurarse de que cumplan con las exigencias y los reglamentos vigentes.

Los bancos deben tener suma cautela al supervisar a los agentes de depósito que no constituyan entidades reguladas y:

- Sean desconocidos para el banco.
- Realicen negocios u obtengan depósitos principalmente en otras jurisdicciones.
- Usen negocios o bancos desconocidos o difíciles de contactar para verificar las referencias.
- Presten otros servicios que puedan ser sospechosos, como la creación de compañías fantasmas para clientes extranjeros.

- Se rehúsen a proporcionar la información de auditoría y debida diligencia solicitada o insistan en colocar depósitos antes de proporcionar dicha información.

- Usen tecnología que proporcione anonimato a los clientes.

Los bancos también deben supervisar las relaciones con los agentes de depósito existentes para detectar cualquier cambio significativo en las estrategias comerciales que pueda tener efecto sobre el perfil de riesgo del agente. Como tales, los bancos deben volver a verificar y actualizar periódicamente los perfiles de cada agente de depósito para garantizar que el análisis de riesgos sea adecuado.

Procedimientos de Inspección

Depósitos mediante agentes

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con respecto a depósitos mediante agentes y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos respecto a las relaciones de depósitos mediante agentes. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades del agente de depósito del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con los depósitos mediante agentes, particularmente aquellas que planteen un mayor riesgo de lavado de dinero.

3. Determine si el sistema del banco para supervisar las relaciones del agente de depósito en busca de actividades sospechosas e informar de actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de depósitos mediante agentes, así como inspecciones previas e informes de auditoría, seleccione una muestra de las cuentas del agente de depósito de mayor riesgo. Cuando seleccionen una muestra, los inspectores deben considerar lo siguiente:

   - Nuevas relaciones con los agentes de depósito.
   - El método de generación de fondos (p. ej., agentes vía Internet).
   - Tipos de clientes (p. ej., clientes no residentes o fuera del país, personalidades sujetas a exposición política o bancos fantasmas extranjeros).
   - Un agente de depósito que haya aparecido en los Informes de actividades sospechosas (SAR).
   - Notificación de citaciones al banco por un agente de depósito en particular.
   - Proveedores de fondos extranjeros.
   - Actividad poco habitual.

6. Revise la información de debida diligencia de los clientes del agente de depósito. Respecto a los agentes de depósitos que son considerados de mayor riesgo (p. ej., solicitan fondos extranjeros, comercializan a través de Internet o son agentes independientes), analice si la siguiente información está disponible:

   - Antecedentes y referencias.
   - Negocios y métodos de comercialización.
   - Prácticas de debida diligencia y aceptación de clientes.
   - El método o fundamento del programa de bonificación o compensación del agente.
   - La fuente de los fondos del agente.
   - Su actividad prevista o tipos y niveles de transacciones (p. ej., transferencias de fondos).

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados a los agentes de depósitos.

Cajeros Automáticos de Propiedad Privada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con cajeros automáticos de propiedad privada (ATM) y Organizaciones de ventas independientes (ISO), y de la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Los cajeros automáticos de propiedad privada son particularmente susceptibles al lavado de dinero y al fraude. Los operadores de estos cajeros automáticos con frecuencia están incluidos en la definición de ISO.[204]

Los cajeros automáticos de propiedad privada generalmente se encuentran en minimercados, bares, restaurantes, tiendas de comestibles o establecimientos de cobro de cheques. Algunas ISO operan a gran escala, por otra parte, los propietarios de muchos cajeros automáticos de propiedad privada son los dueños de los establecimientos en los que están ubicados. La mayoría otorgan dinero en efectivo, mientras que algunos sólo otorgan un recibo impreso (vale) que el cliente cambia por dinero o mercadería. Los honorarios y recargos por las extracciones, junto a los negocios adicionales generados por el acceso de un cliente a un cajero automático, hacen que operar un cajero automático de propiedad privada sea rentable.

Las ISO vinculan sus cajeros automáticos a una red de transacciones de cajeros automáticos. Esta red envía los datos de las transacciones al banco del cliente para debitarlos de la cuenta de éste y finalmente acreditar los montos a la cuenta de la ISO, que puede estar ubicada en cualquier banco del mundo. Por lo general, los pagos a la cuenta de la ISO se hacen a través del sistema ACH. Más información sobre los tipos de sistemas de pago de operaciones al por menor está disponible en el manual *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC[205]

Banco patrocinador

Algunas transferencias electrónicas de fondos (EFT, por su siglas en inglés) o redes de puntos de venta (POS) requieren que la ISO esté patrocinada por algún miembro de la red (banco patrocinador). El banco patrocinador y la ISO están sujetos a todas las normas de

[204] Una ISO generalmente actúa como agente de los intermediarios, incluidos los propietarios de los cajeros automáticos, para procesar transacciones electrónicas. En algunos casos, el propietario de un cajero automático puede actuar como su propio procesador ISO. Los bancos pueden contratar los servicios de una ISO para buscar intermediarios y cajeros automáticos de propiedad privada; sin embargo, en muchas situaciones, las ISO contratan con los intermediarios y los propietarios de los cajeros automáticos sin el control ni la aprobación del banco de compensación.

[205] El *Information Technology Examination Handbook* (Manual para el examen de tecnología de información) del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

la red. El banco patrocinador también está encargado de garantizar que la ISO cumpla con todas las normas de la red. Por lo tanto, el banco patrocinador debe realizar una debida diligencia apropiada a la ISO y mantener la documentación adecuada para asegurar que la ISO patrocinada cumpla con las normas de la red.

Factores de riesgo

Actualmente, la mayoría de los estados no registra, no establece límites a la propiedad, como tampoco supervisa o inspecciona los cajeros automáticos de propiedad privada ni a sus ISO.[206] Si bien el proveedor de la red de transacciones de cajeros automáticos y el banco patrocinador deberían llevar a cabo la debida diligencia con respecto a las ISO, en la práctica esto puede variar. Además, es posible que el prestador no se entere de los cambios que se produzcan en la propiedad del ATM o de la ISO una vez que el contrato de ATM haya entrado en vigencia. Como resultado, muchos cajeros automáticos de propiedad privada han participado en estratagemas de lavado de dinero, robo de identidad, robo directo del dinero del ATM y fraude, o son vulnerables a la comisión de los mencionados delitos. Por lo tanto, los cajeros automáticos de propiedad privada y sus ISO implican un mayor riesgo y deben ser tratados en consecuencia por los bancos que negocian con ellos.

La debida diligencia comienza a ser un desafío mayor cuando las ISO venden cajeros automáticos a compañías de tercer y cuarto nivel ("sub-ISO") cuya existencia puede ser desconocida por el banco patrocinador, o realizan una subcontratación con dichas compañías. Cuando una ISO contrata o vende cajeros automáticos a una sub-ISO, el banco patrocinador puede desconocer quién es realmente el dueño del cajero automático. Por ende, las sub-ISO pueden ser dueñas y operar cajeros automáticos que permanezcan virtualmente invisibles al banco patrocinador.

Algunos cajeros automáticos de propiedad privada son administrados por servidores de efectivo para bóvedas, los cuales transportan el dinero en un vehículo blindado, reabastecen los cajeros automáticos, y los aseguran contra robos y daños. Sin embargo, muchas ISO administran y mantienen a sus propias máquinas, e incluso las abastecen con dinero en efectivo. Los bancos también pueden proporcionar dinero a las ISO mediante contratos de préstamo, lo que expone a esos bancos a diferentes riesgos, inclusive el riesgo de afectar su reputación y su crédito.

El lavado de dinero puede ocurrir a través de cajeros automáticos de propiedad privada cuando algunos de éstos se reabastecen con dinero obtenido ilícitamente que luego es retirado por clientes legítimos. Este proceso deriva en depósitos de ACH en la cuenta ISO que aparentan ser transacciones comerciales legítimas. Por lo tanto, las tres fases del lavado

[206] El 3 de Diciembre de 2007, la FinCEN publicó la guía interpretativa *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services* (Aplicación de la definición de negocios de servicios monetarios a determinados propietarios y operadores de cajeros automáticos que ofrecen servicios limitados), FIN-2007-G006, en la cual aclara las circunstancias en las que un propietario, no bancario, y operador de un cajero automático constituiría un negocio de servicios monetarios a los efectos de la Ley de Secreto Bancario y sus reglamentos de ejecución.

de dinero (colocación, transformación e integración) pueden darse simultáneamente. Los lavadores de dinero pueden también confabularse con los intermediarios y las ISO que antes eran legítimas, para abastecer los cajeros automáticos con dinero ilícito a cambio de un descuento.

Mitigación del riesgo

Los bancos deben implementar políticas, procedimientos y procesos apropiados, que incluyan debida diligencia adecuada y supervisión de actividades sospechosas, para tratar los riesgos que presentan los clientes ISO. Como mínimo, estas políticas, procedimientos y procesos deben incluir:

- Debida diligencia adecuada en función del riesgo respecto a la ISO, mediante un control de la documentación, las licencias, los permisos, los contratos o las referencias de la corporación.
- Control de las bases de datos públicas para identificar problemas o preocupaciones potenciales relacionados con la ISO o sus propietarios principales.
- La comprensión de los controles de la ISO sobre los acuerdos para el suministro de dinero a los ATM de propiedad privada, incluida la fuente de reabastecimiento de las máquinas.
- Documentación de la ubicación de los cajeros automáticos de propiedad privada y determinación del mercado geográfico objetivo de la ISO.
- Actividad prevista de la cuenta, incluidas las extracciones de dinero en efectivo.

A causa de estos riesgos, es fundamental realizar una debida diligencia a las ISO que vaya más allá de las exigencias mínimas del CIP. Los bancos también deben realizar la debida diligencia a los propietarios de los cajeros automáticos y a las sub-ISO, según sea pertinente. Esta debida diligencia puede incluir:

- El control de la documentación, las licencias, los permisos, los contratos o las referencias de la corporación, incluido el contrato de prestación de transacciones del ATM
- El control de las bases de datos públicas en busca de información sobre los propietarios de los cajeros automáticos.
- La obtención de las direcciones de todas las ubicaciones de los cajeros automáticos, determinando los tipos de negocios donde estén ubicados, e identificando la población objetivo.
- La determinación de los niveles de actividad previstos del cajero automático, incluidas las extracciones de dinero.
- La determinación de las fuentes de dinero en efectivo de los cajeros automáticos mediante el control de copias de los contratos con el vehículo blindado, los contratos de préstamos o cualquier otra documentación, según sea pertinente.

- La obtención de información sobre la ISO respecto a la debida diligencia en sus acuerdos sub-ISO, como la cantidad de cajeros automáticos y su ubicación, el volumen de las transacciones, el volumen en dólares y la fuente de reabastecimiento de dinero en efectivo.

Procedimientos de Inspección

Cajeros automáticos de propiedad privada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las relaciones con cajeros automáticos de propiedad privada (ATM) y Organizaciones de ventas independientes (ISO), y de la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de cajeros automáticos de propiedad privada. Evalúe la aptitud de las políticas, los procedimientos y los procesos respecto a las relaciones con los ATM de propiedad privada y las ISO, y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de los cajeros automáticos de propiedad privada.

3. Determine si el sistema del banco para supervisar las cuentas de los cajeros automáticos de propiedad privada en busca de actividades sospechosas, y para informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Determine si el banco patrocina membresías de la red para las ISO. Si el banco es un banco patrocinador, revise los acuerdos contractuales con las redes y las ISO para determinar si los procedimientos y los controles de debida diligencia están diseñados para garantizar que las ISO cumplen con las normas de red. Determine si el banco obtiene información de las ISO con respecto a la debida diligencia en sus acuerdos sub-ISO.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus relaciones con cajeros automáticos de propiedad privada y con las ISO, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de cajeros automáticos de propiedad privada. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la información referente a la CDD del banco. Determine si la información verifica de manera adecuada la identidad de las ISO y describe:

     – Sus antecedentes.

     – La fuente de sus fondos.

     – Su actividad prevista o tipos y niveles de transacciones (p. ej., transferencias de fondos).

- Sus ATM (tamaño y ubicación).
- Su acuerdo de entrega de dinero en efectivo, de ser aplicable.

- Revise cualquier informe MIS que el banco utilice para supervisar las cuentas ISO. Determine si el flujo de fondos o la actividad prevista es coherente con la información de CDD.

6. Determine si una ISO patrocinada utiliza proveedores o prestadores de servicios externos para cargar dinero, mantener los cajeros automáticos o solicitar ubicaciones de intermediarios. De ser así, revise una muestra de los acuerdos de servicios externos para verificar la aplicación de procedimientos de debida diligencia y control adecuados.
7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las ISO.

Productos de Inversión que no son para Depositar: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con productos de inversión que no son para depositar (NDIP, por sus siglas en inglés) internos y en red, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Los NDIP incluyen un amplio rango de productos de inversión (p. ej., valores, bonos, y rentas vitalicias fijas o variables). Los programas de venta también pueden incluir cuentas de administración de dinero en efectivo con servicio de barrido para clientes minoristas y comerciales; los bancos ofrecen esto programas directamente. Los bancos ofrecen estas inversiones para aumentar sus ingresos por honorarios y proporcionar a los clientes productos y servicios adicionales. La manera en que está estructurada la relación con los NDIP y los métodos mediante los cuales se ofrecen, afecta sustancialmente los riesgos y responsabilidades BSA/AML del banco.

Acuerdos de operación en red

Los bancos generalmente realizan acuerdos de operación en red con agentes bursatiles para ofrecer NDIP en las instalaciones del banco. A los efectos de BSA/AML, bajo un acuerdo de operación en red el cliente es cliente del agente de valores o de bolsa, aunque también puede ser cliente del banco respecto a otros servicios financieros. Los inspectores del banco reconocen que la Comisión de Valores y Bolsa de los EE. UU. (SEC, por sus siglas en inglés) es el principal regulador de la oferta de NDIP por medio de agentes bursatiles, y las agencias observarán las exigencias de supervisión funcional de la Ley Gramm–Leach–Bliley.[207] Las agencias bancarias federales están encargadas de supervisar las actividades NDIP realizadas directamente por los bancos. Los diferentes tipos de acuerdos de operación en red pueden incluir productos de marca conjunta, acuerdos para compartir empleados o acuerdos con terceros.

[207] La regulación funcional limita las circunstancias en las cuales las agencias bancarias federales pueden inspeccionar directamente o exigir informes de una subsidiaria o filial bancaria cuyo regulador principal es la SEC, la Comisión de Operaciones de Futuros Productos o las autoridades estatales de emisión. Las agencias bancarias federales por lo general tienen vedada la inspeccionar de esas entidades, a menos que se requiera más información para determinar si la subsidiaria o filial bancaria representa un riesgo material para el banco, para determinar el cumplimiento de alguna a exigencia legal bajo la jurisdicción de la agencia bancaria federal, o para analizar el sistema de gestión de riesgos del banco que cubre las actividades funcionalmente reguladas. Estos estándares requieren mayor dependencia del regulador funcional y más colaboración entre los reguladores.

Productos de marca conjunta

Los productos de marca conjunta son ofrecidos por otra empresa o corporación de servicios financieros[208] en patrocinio conjunto con el banco. Por ejemplo, una corporación de servicios financieros adapta un producto de fondo común para la venta en un banco específico. El producto es vendido exclusivamente en ese banco y lleva el nombre tanto del banco como de la corporación de servicios financieros.

Debido a esta relación de marca conjunta, la responsabilidad del cumplimiento con BSA/AML se vuelve conjunta. Puesto que estas cuentas no están únicamente bajo el control del banco o de la entidad financiera, puede variar la responsabilidad de llevar a cabo el CIP, la CDD, y la supervisión y el informe de actividades sospechosas. El banco debe conocer plenamente las responsabilidades contractuales de cada parte y garantizar que todas las partes realicen los controles adecuados.

Acuerdos para compartir empleados

En un acuerdo para compartir empleados, el banco y una corporación de servicios financieros, como una agencia de seguros o un agente de valores o de bolsa registrado, tienen un empleado en común (compartido). El empleado compartido puede encargarse de realizar negocios bancarios y también de vender NDIP, o bien vender NDIP a tiempo completo. Debido a este acuerdo para compartir empleados, el banco conserva sus responsabilidades respecto a las actividades relacionadas con los NDIP. Incluso en el caso de que los acuerdos contractuales establezcan que la corporación de servicios financieros será responsable del cumplimiento BSA/AML, el banco debe garantizar una supervisión adecuada de todos sus empleados, incluidos los empleados compartidos, y su cumplimiento con todas las exigencias normativas.[209]

Bajo algunos acuerdos de operación en red, los representantes registrados de ventas de valores son empleados compartidos entre el banco y el agente de bolsa o de valores. Cuando el empleado compartido ofrece productos y servicios de inversión, el agente de bolsa o de valores es responsable de supervisar el cumplimiento del representante registrado con la normativa vigente sobre valores aplicable. Cuando el empleado compartido ofrece productos y servicios bancarios, el banco tiene la responsabilidad de supervisar el desempeño del empleado y su cumplimiento con la BSA/AML.

Acuerdos con un tercero

Los acuerdos con terceros pueden comprender el alquiler del espacio que se encuentra en el vestíbulo del banco a una corporación de servicios financieros para vender NDIP. En

---

[208] Una corporación de servicios financieros incluye a aquellas entidades que ofrecen NDIP, que pueden ser, por ejemplo, empresas de inversión, instituciones financieras, agentes bursatiles, y compañías de seguros.

[209] Si el banco aplica la disposición sobre dependencia del CIP, la responsabilidad por el CIP se traslada al proveedor externo. Consulte la sección del esquema general principal, “Programa de identificación de clientes” en las páginas 57 a 64, para obtener información adicional.

este caso, el tercero debe diferenciarse a sí mismo claramente del banco. Si el acuerdo se implementa correctamente, los acuerdos con terceros no afectan las exigencias de cumplimiento BSA/AML del banco. Como una práctica responsable, se recomienda a los bancos comprobar si el prestador de servicios financieros cuenta con un programa de cumplimiento BSA/AML adecuado como parte de su debida diligencia.

Ventas realizadas internamente y productos de propiedad exclusiva

A diferencia de los acuerdos de operación en red, el banco es plenamente responsable por las transacciones NDIP realizadas internamente a nombre de sus clientes, impliquen o no el beneficio de un empleado interno del agente de bolsa o de valores.[210] Además, el banco también puede ofrecer sus NDIP de propiedad exclusiva, los cuales pueden ser creados y ofrecidos por el banco, su subsidiaria o una filial.

Con respecto a las ventas realizadas internamente y los productos de propiedad exclusiva, es posible que la totalidad de las relaciones con el cliente y todos los riesgos BSA/AML deban ser gestionados por el banco, según la manera en que se vendan los productos. A diferencia de los acuerdos de operación en red, en los cuales todas o algunas responsabilidades pueden ser asumidas por el agente de bolsa o de valores de terceros respecto a ventas realizadas internamente y productos de propiedad exclusiva, el banco debe gestionar todo lo relativo a las ventas de NDIP realizadas internamente y de NDIP de propiedad exclusiva, no sólo en todos sus departamentos, sino en toda la institución.

Factores de riesgo

Los riesgos BSA/AML se presentan porque los NDIP pueden implicar acuerdos legales complejos, grandes volúmenes en dólares y rápidos movimientos de fondos. Las carteras NDIP que administran y controlan directamente los clientes plantean un mayor riesgo de lavado de dinero que los que administran los bancos o prestadores de servicios financieros. Los clientes experimentados pueden llegar a estructurar sus propiedades de tal forma que queden ocultos la propiedad y el control finales de estas inversiones. Por ejemplo, los clientes pueden conservar cierto nivel de anonimato constituyendo Compañías de inversión privada (PIC),[211] fideicomisos fuera del país u otras entidades de inversión que oculten su propiedad o derecho de usufructo.

---

[210] En algunas circunstancias, no se considerará a los bancos como agentes de bolsa o de valores, y no se requerirá que el empleado sea registrado como agente de bolsa o de valores. Para ver una lista completa, consulte 15 USC 78c(a)(4).

[211] Consulte la sección del esquema general ampliado, “Entidades comerciales (nacionales y extranjeras)”, en las páginas 357 a 364, como guía para las PIC.

Mitigación del riesgo

La gerencia debe desarrollar políticas, procedimientos y procesos en función del riesgo, que le permitan al banco identificar relaciones y circunstancias de cuenta poco habituales, activos y fuentes de fondos cuestionables y otras áreas potenciales de riesgo (p. ej., cuentas fuera del país, cuentas en agencias y beneficiarios no identificados). La gerencia debe mantenerse alerta a las situaciones que requieran un control o una investigación adicional.

Acuerdos de operación en red

Antes de establecer un acuerdo de operación en red, los bancos deben realizar un control adecuado del agente de bolsa o de valores. El control debe incluir un análisis del estado financiero del mismo y de su experiencia gerencial, del carácter de su vinculación con la Asociación Nacional de Operadores de Valores o Bolsa (NASD, por sus siglas en inglés), de su reputación y de su capacidad para observar las responsabilidades de cumplimiento BSA/AML con respecto a los clientes del banco. Una debida diligencia adecuada debería incluir la determinación de que el agente de bolsa o de valores cuenta con políticas, procedimientos y procesos adecuados para cumplir con sus obligaciones legales. El banco debe mantener documentación sobre la debida diligencia del agente de bolsa o de valores. Además, todos los aspectos relacionados con las responsabilidades BSA/AML del agente de bolsa o de valores y de sus representantes registrados, incluyendo las relativas a la supervisión e informe de actividades sospechosas, deben estar contempladas en detalle en contratos escritos.

Un banco también puede querer mitigar su exposición al riesgo limitando ciertos productos de inversión ofrecidos a sus clientes. Los productos de inversión tales como las PIC, los fideicomisos, o los fondos de cobertura fuera del país, pueden implicar transferencias internacionales de fondos u ofrecer a los clientes formas de ocultar la titularidad de las propiedades.

La gerencia del banco debe hacer esfuerzos razonables para actualizar la información de debida diligencia de los agentes de bolsa o de valores. Dichos esfuerzos pueden incluir controles periódicos de la información sobre el cumplimiento de los agentes de bolsa o de valores con sus responsabilidades BSA/AML, verificación de sus antecedentes de cumplimiento con los requisitos de las pruebas y un control de las quejas de los clientes. También se recomienda a la gerencia, siempre que sea posible, controlar los informes BSA/AML generados por el agente de bolsa o de valores. Este control puede incluir información sobre apertura de cuentas, transacciones, productos de inversión vendidos y supervisión e informe de actividades sospechosas.

Ventas realizadas internamente y productos de propiedad exclusiva

La gerencia del banco debe analizar el riesgo considerando diferentes factores tales como:

- Tipo de NDIP comprados y el tamaño de las transacciones.
- Los tipos y la frecuencia de las transacciones.

- País de residencia de los mandantes o beneficiarios, o el país de constitución, o la fuente de los fondos.
- Las cuentas y transacciones que no sean habituales o acostumbradas para el cliente o el banco.

Respecto a los clientes que la gerencia considera de mayor riesgo de lavado de dinero y financiamiento del terrorismo, se deben establecer requisitos de documentación más estrictos, verificación y procedimientos de supervisión de las transacciones. Posiblemente sea adecuado llevar a cabo una EDD en las siguientes situaciones:

- Al iniciar el banco una relación con un cliente nuevo.
- Cuando las cuentas no discrecionales registren activos cuantiosos o transacciones frecuentes.
- El cliente reside en una jurisdicción extranjera.
- El cliente es una PIC u otra estructura corporativa establecida en una jurisdicción de mayor riesgo.
- Los activos y las transacciones son atípicas para el cliente.
- El tipo de inversiones, el tamaño, los activos o las transacciones son atípicas para el banco.
- Las transferencias internacionales de fondos se realizan especialmente desde fuentes de fondos ubicadas fuera del país.
- Las identidades de los mandantes o beneficiarios de inversiones o relaciones no se conocen o no se pueden determinar fácilmente.
- Las personalidades sujetas a exposición política (PEP) son parte en las inversiones o transacciones.

Procedimientos de Inspección

Productos de inversión que no son para depositar

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con productos de inversión que no son para depositar (NDIP, por sus siglas en inglés) internos y en red, y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los NDIP. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades con NDIP del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Si procede, revise los acuerdos contractuales con prestadores de servicios financieros. Determine la responsabilidad en el cumplimiento BSA/AML de cada parte. Determine si estos acuerdos proporcionan una supervisión BSA/AML adecuada.

3. A partir de un control de los informes de los MIS (p. ej., informes de excepciones, informes de transferencias de fondos e informes de supervisión de actividades) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz los NDIP, particularmente aquellos que planteen un mayor riesgo de lavado de dinero.

4. Determine de qué manera incluye el banco las actividades de ventas de NDIP en sus sistemas de acumulación BSA/AML aplicables a todo el banco o, según corresponda, a toda la institución.

5. Determine si el sistema del banco para supervisar los NDIP e informar sobre actividades sospechosas es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

Si el banco o su subsidiaria de participación mayoritaria son responsables de la venta o supervisión directa de los NDIP, los inspectores deben llevar a cabo los siguientes procedimientos de prueba de transacciones en las cuentas de clientes establecidas por el banco:

7. En función del análisis de riesgos del banco de sus actividades con NDIP, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los NDIP de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

- Revise la documentación adecuada, incluidos los CIP, para asegurarse de que se haya practicado la debida diligencia adecuada y se hayan mantenido los registros adecuados.
- Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones para verificar:
  - Las transacciones previstas con la actividad real.
  - Conjunto de activos que excedan el valor neto del cliente.
  - Patrones de operaciones bursátiles irregulares (p. ej., transferencias de fondos entrantes para comprar valores seguidas de la entrega de los valores a otro custodio poco tiempo después).
- Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado de la cuenta. Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de ventas de NDIP.

Seguros: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la venta de productos de seguros cubiertos y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Los bancos venden seguros para aumentar su rentabilidad, principalmente a través de la ampliación y diversificación de los ingresos por servicios. Generalmente, los productos de seguros se venden a los clientes del banco a través de acuerdos en red con una filial, una subsidiaria en operación u otros proveedores externos de seguros. Los bancos también están interesados en proporcionar oportunidades de ventas cruzadas para los clientes ampliando los productos de seguros que ofrecen. Por lo general, los bancos asumen el papel de agente de terceros en la venta de productos de seguros cubiertos. Los tipos de productos de seguros vendidos pueden incluir los de vida, médico, sobre la propiedad, contra accidentes, y de renta vitalicia fija o variable.

Exigencias de presentación de informes de actividades sospechosas y de programas de cumplimiento AML para compañías de seguros

Las normas de la FinCEN imponen a las compañías de seguros exigencias del programa de cumplimiento AML y obligaciones con respecto a los SAR similares a las impuestas a los bancos.[212] Los reglamentos sobre los seguros se aplican sólo a las compañías de seguros; no existen obligaciones independientes para los productores y agentes de seguros. Sin embargo, la compañía de seguros es responsable de la realización y eficacia de su programa de cumplimiento AML, que incluye las actividades de productores y agentes. Los reglamentos de seguros sólo son aplicables a un rango limitado de productos que pueden plantear un mayor riesgo de abuso por parte de los lavadores de dinero y los financistas del terrorismo. Un producto cubierto, a los efectos de un programa de cumplimiento AML, es:

- Una póliza de seguro de vida permanente, que no sea una póliza de seguro de vida grupal.
- Cualquier contrato de renta vitalicia, que no sea un contrato de renta vitalicia grupal.
- Cualquier otro producto de seguros con servicios de valor de contado o inversión.

Cuando se le exige a un agente o productor de seguros establecer un programa de cumplimiento BSA/AML bajo otra exigencia de los reglamentos de la BSA (p. ej., las exigencias para los agentes de valores o del banco), generalmente la compañía de seguros puede depender de ese programa de cumplimiento para ocuparse de los asuntos en el

[212] 31 CFR 103.137 y 31 CFR 103.16.

momento de la venta del producto cubierto.[213] Sin embargo, el banco puede necesitar establecer políticas, procedimientos y procesos específicos para sus ventas de seguros a fin de enviar la información a la compañía de seguros para que ésta cumpla con el programa AML.

Asimismo, si un banco, como agente de la compañía de seguros, detecta actividades sospechosas o poco habituales relacionadas con las ventas de seguros, puede presentar un SAR en conjunto con la compañía de seguros sobre la actividad en común.[214]

En Abril de 2008, la FinCEN publicó un informe analítico y estratégico que proporciona información sobre determinadas tendencias, patrones y tipologías de lavado de dinero en relación con los productos de seguros. Consulte *Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings* (Informes de actividades sospechosas en la industria de los seguros: Una evaluación de las presentaciones de informes de actividades sospechosas), en www.fincen.gov.

Factores de riesgo

Los productos de seguros se pueden utilizar para facilitar el lavado de dinero. Por ejemplo, se puede utilizar dinero para comprar una o más pólizas de seguro de vida, que un asegurado posteriormente puede cancelar rápidamente (también conocida como "amortización anticipada") siendo pasible de una sanción. La compañía de seguros reembolsa el dinero al comprador en la forma de un cheque. Las pólizas de seguro sin servicios de valor de contado o inversión plantean riesgos menores, pero pueden utilizarse para lavar dinero o financiar el terrorismo a través de la presentación de quejas falsas o exageradas por parte del asegurado a su compañía aseguradora, que de ser pagadas, permitirían al asegurado recuperar una parte o la totalidad de los pagos otorgados originalmente. Otras maneras en que se pueden utilizar los productos de seguros para lavar dinero incluyen:

- Pedir prestado el valor de rescate de las pólizas de seguro de vida permanentes.
- Vender unidades en productos vinculados con inversiones (como renta vitalicia).

---

[213] 70 Registro Federal 66758 (3 de Noviembre de 2005). Consulte también la Guía del FFIEC FIN-2006-G015, las *Frequently Asked Question, Customer Identification Programs and Banks Serving as Insurance Agents*, (Preguntas frecuentes, los Programas de identificación de clientes y Bancos que prestan servicios como agentes de seguros), del 12 de Diciembre de 2006, en www.fincen.gov/final_bank_insurance_agent_faq_12122006.pdf.

[214] La FinCEN ha publicado un documento de preguntas frecuentes, *Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies* (Exigencias de presentación de informes de actividades sospechosas y programa antilavado de dinero para compañías de seguros), en (www.fincen.gov)). A menos que el formulario del SAR incorpore múltiples responsables de la presentación del informe, sólo una institución se identifica como la responsable de la presentación del informe en la sección "*Filer Identification*" (Identificación del responsable de la presentación del informe) del formulario del SAR. En esos casos, la descripción debe incluir las palabras "*joint filing*" (presentación del informe en conjunto) e identificar a las otras instituciones en nombre de las cuales se presenta el informe.

- Utilizar ingresos de seguros provenientes de una amortización anticipada de la póliza para comprar otros activos financieros.
- Comprar pólizas que permitan la transferencia de derechos de usufructo sin el conocimiento ni el consentimiento del emisor (p. ej., póliza de seguro total de segunda mano y pólizas de seguros al portador).[215]
- Comprar productos de seguros a través de métodos poco habituales como moneda o equivalentes a la moneda.
- Comprar productos con servicios de interrupción del seguro sin tener en cuenta el rendimiento de la inversión del producto.

Mitigación del riesgo

Para mitigar los riesgos del lavado de dinero, el banco debe adoptar políticas, procedimientos y procesos que incluyan:

- La identificación de las cuentas de mayor riesgo.
- Debida diligencia de los clientes, incluida la debida diligencia especial para las cuentas de mayor riesgo.
- Diseño y uso del producto, tipos de servicios prestados y aspectos o riesgos particulares que presenten los mercados objetivo.
- Compensación de empleados y acuerdos de bonificación relacionados con las ventas.
- Supervisión, incluido el control de la terminación anticipada de pólizas y la presentación de informes de transacciones sospechosas y poco habituales (p. ej., un pago de prima único y elevado, la compra de un producto por parte de un cliente que parece salirse del rango normal de las transacciones financieras de ese cliente, rescate o redención anticipada, múltiples transacciones, pagos a terceros aparentemente no relacionados y préstamos respaldados con garantía).
- Exigencias en cuanto a la gestión de registros.

---

[215] Consulte *Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* (Documento orientativo contra el lavado de dinero y la lucha contra el financiamiento del terrorismo) de la Asociación Internacional de Supervisores de Seguros, de Octubre de 2004, disponible en www.iaisweb.org.

Procedimientos de Inspección

Seguros

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con la venta de productos de seguros cubiertos y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las ventas de seguros. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de ventas de seguros del banco, su papel en las ventas de seguros y los riesgos que dichas ventas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Revise los contratos y acuerdos para los acuerdos en red del banco con las filiales, subsidiarias en operación u otros proveedores externos de seguros que lleven a cabo actividades de ventas dentro de las instalaciones de un banco y en nombre de éste.

3. Dependiendo de las responsabilidades del banco que se establezcan en los contratos y acuerdos, revise los informes de los MIS (p. ej., informes de grandes volúmenes, pagos únicos de la prima, registros de cancelación anticipada de pólizas, pagos de primas que excedan los valores de éstas y cesiones de derechos sobre pago) y los factores de valoración de riesgos internos. Determine si el banco identifica y supervisa de manera eficaz las ventas de productos de seguros cubiertos.

4. Dependiendo de las responsabilidades del banco que se establezcan en los contratos y acuerdos, determine si el sistema del banco para la supervisión de los productos de seguros cubiertos para detectar y elaborar informes de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

Si el banco o su subsidiaria de participación mayoritaria son responsables de la venta o supervisión directa de los seguros, los inspectores deben llevar a cabo los siguientes procedimientos de prueba de transacciones.

6. En función del análisis de riesgos del banco de sus actividades de ventas de seguros, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de los productos de seguros cubiertos. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.

- Revise la actividad de la cuenta. Compare las transacciones anticipadas con las transacciones reales.
- Determine si la actividad es sospechosa o poco habitual.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las ventas de seguros.

Cuentas de Concentración: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas de concentración y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

Las cuentas de concentración son cuentas internas establecidas para facilitar el procesamiento y liquidación de transacciones múltiples o individuales de los clientes dentro del banco, generalmente el mismo día. Estas cuentas también se conocen como cuentas de uso especial, cuentas ómnibus, cuentas puente o de tránsito, de liquidación, intradía, de barrido o de cobro. A menudo se utilizan para facilitar las transacciones de la banca privada, cuentas fiduciarias y de custodia de valores, transferencias de fondos y filiales internacionales.

Factores de riesgo

El riesgo de lavado de dinero puede surgir en las cuentas de concentración si la información de identificación de clientes —como el nombre, la suma de la transacción y el número de cuenta— se separa de la transacción financiera. Si ocurre la separación, se pierde el rastro de auditoría y es posible que las cuentas se usen o administren de manera indebida. Los bancos que usen cuentas de concentración deben implementar políticas, procedimientos y procesos que cubran la operación y gestión de registros de estas cuentas. Las políticas deben establecer pautas para identificar, medir, supervisar y controlar los riesgos.

Mitigación del riesgo

Debido a los riesgos planteados, la gerencia debe familiarizarse con el tipo de negocio de sus clientes y con las transacciones que pasen por las cuentas de concentración del banco. Además, la supervisión de las transacciones de las cuentas de concentración es necesaria para identificar e informar sobre transacciones sospechosas o poco habituales.

Los controles internos son necesarios para garantizar que las transacciones procesadas incluyan la información de identificación de clientes. La conservación de información completa es esencial para garantizar el cumplimiento con las exigencias normativas y la supervisión adecuada de las transacciones. Los controles internos adecuados pueden incluir:

- Mantener un sistema integral que identifique, en todo el banco, las cuentas del libro mayor utilizadas como cuentas de concentración, así como los departamentos e individuos autorizados para usar esas cuentas.
- Exigir dos firmas en los tiquetes del libro mayor.
- Prohibir a los clientes el acceso directo a las cuentas de concentración.
- Capturar las transacciones de los clientes en los estados de cuenta de los mismos.

- Prohibir que los clientes que tengan conocimiento de las cuentas de concentración o que puedan impartir instrucciones a los empleados para que éstos realicen transacciones a través de esas cuentas.
- Conservar la información adecuada relativa a transacciones e identificación de clientes.
- Asignar a una persona no relacionada con las transacciones para que se encargue de conciliar frecuentemente las cuentas.
- Establecer un proceso oportuno para solucionar discrepancias.
- Identificar los nombres de los clientes habituales.

Procedimientos de Inspección

Cuentas de concentración

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las cuentas de concentración y la capacidad de la gerencia de implementar sistemas eficaces de supervisión e informe.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las cuentas de concentración. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de cuentas de concentración del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de concentración.

3. Revise el libro mayor e identifique todas las cuentas de concentración existentes. Luego de tratar las cuentas de concentración con la gerencia y de realizar investigaciones adicionales necesarias, obtenga y revise una lista de todas las cuentas de concentración y las conciliaciones bancarias más recientes.

4. Determine si el sistema del banco para supervisar las cuentas de concentración, detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de sus actividades de cuentas de concentración, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de concentración. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Obtenga informes de actividad de cuenta relativos a las cuentas de concentración seleccionadas.
   - Evalúe la actividad y seleccione una muestra de las transacciones que pasen por diferentes cuentas de concentración para un control adicional.
   - Concéntrese en la actividad de mayor riesgo (p. ej., transferencias de fondos o compras de instrumentos monetarios) y en las transacciones provenientes de jurisdicciones de mayor riesgo.

7. En función de los procedimientos de inspección realizados, incluidas las pruebas a las transacciones, formule una conclusión sobre la adecuación de las políticas, los procedimientos y los procesos asociados con las cuentas de concentración.

Actividades de Préstamo: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de préstamo y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las actividades de préstamo incluyen, entre otras, bienes inmuebles,[216] financiación del comercio internacional,[217] préstamos garantizados con efectivo, tarjetas de crédito, actividades comerciales agrícolas y de particulares. En las actividades de préstamo pueden intervenir varias partes (p. ej., garantes, firmantes, mandantes o participantes del préstamo).

Factores de riesgo

El hecho de que haya varias partes involucradas puede incrementar el riesgo de lavado de dinero o financiamiento del terrorismo cuando la fuente y el uso de los fondos no son transparentes. Esta falta de transparencia puede generar oportunidades en cualquiera de las tres fases de las operaciones de lavado de dinero o estratagemas de financiamiento del terrorismo. Estas estratagemas pueden incluir lo siguiente:

- Para obtener un préstamo, una persona adquiere un certificado de depósito con fondos ilícitos.
- Los préstamos tienen un propósito ambiguo o ilegal.
- Los préstamos se realizan o se pagan a nombre de un tercero.
- El banco o el cliente intentan eliminar la evidencia escrita sobre el solicitante del préstamo y los fondos ilícitos.
- Se otorgan préstamos a personas que residen fuera de los Estados Unidos, especialmente en jurisdicciones y ubicaciones geográficas de mayor riesgo. Los préstamos también pueden incluir garantías ubicadas fuera de los Estados Unidos.

Mitigación del riesgo

Todos los préstamos se consideran cuentas para los propósitos de los reglamentos del Programa de identificación de clientes (CIP). Respecto a los préstamos que implican mayor riesgo de lavado de dinero y financiamiento del terrorismo, incluidos los préstamos

[216] La FinCEN ha publicado informes analíticos y estratégicos sobre las tendencias y los patrones relacionados con el fraude asociado a los créditos hipotecarios, así como el lavado de dinero a través de bienes inmuebles residenciales y comerciales. Consulte www.fincen.gov/news_room/rp/strategic_analytical.html.

[217] Consulte la sección del esquema principal, “Actividades de financiación del comercio internacional” en las páginas 302 a 307, como guía.

enumerados arriba, el banco debe realizar la debida diligencia de las partes relacionadas con la cuenta (p. ej., garantes, firmantes o mandantes). La debida diligencia adicional que se exige para una actividad de préstamo en particular, variará según los riesgos de BSA/AML que se presenten, pero puede incluir la verificación de referencias, la obtención de referencias de crédito, la verificación de la fuente de las garantías y la obtención de extractos de los estados financieros o de la declaración impositiva del solicitante del crédito, así como de todas o varias de las diversas partes involucradas en el préstamo.

Los bancos deben contar con políticas, procedimientos y procesos para supervisar, identificar e informar de actividades poco habituales o sospechosas. La sofisticación de los sistemas empleados para supervisar la actividad de las cuentas de préstamos debe ser acorde al tamaño y complejidad de la actividad de préstamos del banco. Por ejemplo, los bancos pueden controlar los informes de préstamos tales como pagos anticipados, cuentas morosas, fraude o préstamos garantizados con efectivo.

Procedimientos de Inspección

Actividades de préstamo

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de préstamo y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a los préstamos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de préstamo del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las cuentas de préstamos de mayor riesgo.

3. Determine si el sistema del banco para supervisar las cuentas de préstamos, detectar e informar de actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

4. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

5. En función del análisis de riesgos del banco de sus actividades de préstamo, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las cuentas de préstamos de mayor riesgo. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluidos los CIP, para asegurarse de que se haya llevado a cabo la debida diligencia adecuada y mantenido los registros adecuados.

   - Revise, según sea necesario, los antecedentes de préstamo.

   - Compare las transacciones previstas con la actividad real.

   - Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado del préstamo. Identifique cualquier actividad sospechosa o poco habitual.

6. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de préstamos.

Actividades de Financiación del Comercio Internacional: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de financiación del comercio internacional y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

La financiación del comercio internacional, generalmente comprende la financiación a corto plazo para facilitar la importación y exportación de bienes. Estas operaciones pueden incluir el pago si se cumplen las exigencias documentales (p. ej., carta de crédito), o incluir únicamente el pago si el deudor originario no cumple con los términos comerciales de las transacciones (p. ej., garantías o cartas de crédito contingentes). En ambos casos, la participación del banco en la financiación del comercio internacional minimiza los riesgos de la falta de pago tanto para importadores como para exportadores. Sin embargo, el carácter de las actividades de financiación del comercio internacional, exige participación activa de varias partes en ambos extremos de la transacción. Además de la relación básica entre exportador e importador, que está en el centro de toda actividad particular de comercio internacional, pueden existir relaciones entre el exportador y los proveedores, y entre el importador y sus clientes.

Tanto el exportador como el importador pueden tener otras relaciones bancarias. Asimismo, muchas otras instituciones intermediarias financieras y no financieras pueden proporcionar servicios y canales para agilizar los documentos subyacentes y los flujos de pago asociados con las transacciones de comercio internacional. Los bancos pueden participar en la financiación del comercio internacional proporcionando financiación previa a la exportación, ayudando en el proceso de cobro, confirmando o emitiendo cartas de crédito, descontando giros y aprobaciones u ofreciendo servicios por los que se abonan honorarios, tales como brindar información sobre el país y el crédito de los compradores; entre otras alternativas. A pesar de que, en su mayoría, la financiación del comercio internacional es a corto plazo y de carácter autoliquidable, los préstamos a mediano plazo (uno a cinco años) o a largo plazo (más de cinco años) pueden utilizarse para financiar la importación y exportación de bienes de inversión como maquinarias y equipos.

En las transacciones cubiertas por cartas de crédito, los participantes pueden desempeñar los siguientes papeles:

- **Solicitante.** El comprador o la parte que solicita la emisión de una carta de crédito.
- **Banco emisor.** El banco que emite la carta de crédito en nombre del Solicitante y notifica al respecto al Beneficiario, ya sea directamente o a través de un Banco notificador. El Solicitante es cliente del Banco emisor.
- **Banco confirmador.** Generalmente en el país de origen del Beneficiario, a pedido del Banco emisor, el banco que aporta su compromiso de respetar los retiros realizados por el Beneficiario, siempre que se cumplan los términos y las condiciones de la carta de crédito.

- **Banco notificador.** El banco que notifica el crédito ante la solicitud del Banco emisor. El Banco emisor envía el crédito original al Banco notificador para que lo remita al Beneficiario. El Banco notificador autentica el crédito y notifica al respecto al Beneficiario. En una transacción que involucra una carta de crédito pueden intervenir más de un Banco notificador. El Banco notificador también puede ser un Banco confirmador.

- **Beneficiario.** El vendedor o la parte a quien se dirige la carta de crédito.

- **Negociación.** La adquisición por parte del banco designado de giros (librados en otro banco que no sea el banco designado) o documentos presentados conforme a los términos y condiciones del crédito, mediante el adelanto efectivo o el acuerdo de proporcionar un adelanto de los fondos al beneficiario antes o el mismo día hábil en que debe realizarse el reembolso al banco designado.

- **Banco designado.** El banco en el cual el crédito está disponible o cualquier banco en el caso de un crédito disponible en cualquier banco.

- **Banco aceptante.** El banco que acepta un giro, siempre y cuando el crédito exija realizar un giro. Los giros son librados en el Banco aceptante, que pone fecha y firma el instrumento.

- **Banco de descuentos.** El banco que descuenta un giro para el Beneficiario luego de que el Banco notificador lo haya aceptado. Generalmente, el Banco de descuentos es el Banco aceptante.

- **Banco de reembolso.** El banco autorizado por el Banco emisor a reembolsar al Banco pagador presentando reclamos en virtud de la carta de crédito.

- **Banco pagador.** El banco que realiza el pago al Beneficiario de la carta de crédito.

A manera de ejemplo, en un acuerdo de carta de crédito, el banco puede servir como Banco emisor y permitir a su cliente (el comprador) adquirir bienes en el país o el extranjero, o puede actuar como Banco notificador y permitir a su cliente (el exportador) vender sus artículos en el país o el extranjero. La relación entre los dos bancos puede variar y en algunos casos puede incluir cualquiera de las funciones de la lista anterior.

Factores de riesgo

El sistema del comercio internacional está sujeto a una amplia variedad de riesgos y susceptibilidades que ofrecen a las organizaciones criminales la oportunidad de lavar las ganancias provenientes de las actividades delictivas y desplazar los fondos a las organizaciones terroristas con un riesgo de detección relativamente bajo.[218] La

[218] Consulte el informe del Grupo de Acción Financiera sobre *Trade Based Money Laundering* (Lavado de dinero a través de transacciones), del 23 Junio de 2006, en www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

intervención de varias partes a ambos lados de cualquier transacción de financiación del comercio internacional puede dificultar aun más el proceso de la debida diligencia. Además, como el negocio de la financiación del comercio internacional puede depender más de documentos que otras actividades bancarias, puede ser susceptible a la falsificación de documentos, que puede estar relacionada con el lavado de dinero, el financiamiento del terrorismo o con intentos por evitar sanciones de la OFAC u otras restricciones (p. ej., restricciones de exportación, exigencias de licencias o controles).

A pesar de que los bancos deben estar alertas a las transacciones de bienes de mayor riesgo (p. ej., comercio de armas o equipos nucleares), deben tener en cuenta que los bienes pueden estar sobrevalorados o subvalorados para evadir los reglamentos AML o aduaneros, o para transferir los fondos o valores fuera de las fronteras nacionales. Por ejemplo, un importador puede pagar una alta suma de dinero con ingresos provenientes de actividades ilícitas para adquirir bienes que esencialmente carecen de valor y posteriormente son desechados. Como alternativa, los documentos del comercio internacional, como las facturas, pueden ser adulterados mediante fraude para ocultar el engaño. Las variaciones sobre este tema incluyen facturas dobles o incorrectas, envío parcial de bienes (envío incompleto) y el uso de bienes ficticios. Los fondos ilegales transferidos en dichas transacciones consecuentemente aparecen blanqueados e ingresan al terreno del comercio legítimo. Además, en muchas transacciones sospechosas de financiación del comercio internacional también media connivencia entre compradores y vendedores.

La verdadera identidad o titularidad del Solicitante puede encubrirse mediante la adopción de determinadas formas corporativas, como las compañías fantasma o las compañías testaferro emplazadas en el extranjero. La adopción de estos tipos de entidades deriva en una falta de transparencia, ocultando la identidad de la parte compradora de manera eficaz e incrementando así el riesgo de actividad de lavado de dinero y el financiamiento de actividades terroristas.

Mitigación del riesgo

Se deben practicar procedimientos responsables de debida diligencia de los clientes (CDD) para obtener una comprensión exhaustiva del negocio subyacente del cliente y las ubicaciones a las que se prestan servicios. En el proceso relacionado con la carta de crédito, los bancos deben aplicar niveles variables de debida diligencia según su papel en la transacción. Por ejemplo, los Bancos emisores deben llevar a cabo una debida diligencia suficiente con respecto a los posibles clientes antes de otorgar la carta de crédito. La debida diligencia debe incluir la obtención de suficiente información sobre los Solicitantes y Beneficiarios, que incluye su identidad, el carácter del negocio y las fuentes de los fondos. Esto puede requerir la verificación de antecedentes o la realización de investigaciones, especialmente en las jurisdicciones de mayor riesgo. Como tales, los bancos deben realizar un control exhaustivo y conocer de manera razonable a sus clientes antes de facilitar actividades relacionadas con el comercio internacional, y deben comprender exhaustivamente la documentación sobre financiación del comercio internacional. Consulte la sección del esquema general principal, “Debida diligencia de los clientes” en las páginas 69 a 71, como guía.

Del mismo modo, la orientación provista por el *Financial Action Task Force on Money Laundering* (Grupo de Acción Financiera en Contra del Lavado de Dinero; FATF) ha contribuido a establecer importantes normas concernientes a la industria y constituye un recurso para los bancos que prestan servicios de financiación del comercio internacional.[219] El Grupo Wolfsberg también ha publicado pautas y normas propuestas, concernientes a la industria, para los bancos que prestan servicios de financiación del comercio internacional.[220]

Los bancos que desempeñan otros papeles en el proceso relacionado con la carta de crédito deben realizar debida diligencias acorde con sus papeles en cada transacción. Los bancos deben tener en cuenta que, debido a la frecuencia de las transacciones en las que participan varios bancos, los Bancos emisores pueden no tener siempre relaciones corresponsales con el Banco confirmador o notificador.

En la medida de lo posible, los bancos deben revisar la documentación, no sólo para verificar el cumplimiento con las condiciones de la carta de crédito, sino también en busca de anomalías o señales de advertencia que puedan indicar actividades sospechosas o poco habituales. La documentación confiable es fundamental para identificar actividad sospechosa potencial. Al analizar las transacciones de comercio internacional a fin de detectar actividades irregulares o sospechosas, los bancos deben considerar obtener copias de los formularios oficiales de importación y exportación del gobierno extranjero o de los Estados Unidos para evaluar la confiabilidad de la documentación proporcionada.[221] Estas anomalías pueden aparecer en la documentación de envío, fijación irregular de precios evidente, licencias del gobierno (cuando se exijan) o discrepancias en la descripción de los bienes en diversos documentos. La identificación de estos elementos puede, en sí misma, no exigir la presentación de un Informe de actividades sospechosas (SAR), pero puede sugerir la necesidad de una investigación y verificación adicionales. En circunstancias donde se requiera un SAR, no se espera que el banco detenga el comercio internacional ni que interrumpa el procesamiento de la transacción. Sin embargo, se puede requerir detener la transacción para evitar una violación potencial a una sanción de la OFAC.

Con frecuencia, las transacciones de financiación de comercio internacional utilizan mensajes de la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés). Los bancos estadounidenses deben cumplir

---

[219] Consulte *Trade Based Money Laundering*, (Lavado de dinero a través de transacciones), del 23 Junio de 2006, en www.fatf-gafi.org/dataoecd/60/25/37038272.pdf.

[220] Consulte *The Wolfsberg Trade Finance Principles* (Principios de financiación del comercio internacional del Grupo Wolfsberg), de Enero de 2009, en www.wolfsberg-principles.com/pdf/WG_Trade_Finance_Principles_Final_(Jan_09).pdf.

[221] Por ejemplo, el Formulario 7501 de la Oficina de Aduanas y Protección de las Fronteras de los Estados Unidos (Sumario) (http://forms.cbp.gov/pdf/CBP_Form_7501.pdf) y el Formulario 7525-V del Departamento de Comercio de los Estados Unidos (Declaración de exportación de embarque) (www.census.gov/foreign-trade/regulations/forms/new-7525v.pdf) clasifican todas las exportaciones e importaciones estadounidenses mediante códigos de 10 dígitos combinados. (Consulte el www.census.gov/foreign-trade/faq/sb/sb0008.html como guía.)

con los reglamentos de la OFAC, y, cuando sea necesario, expedir licencias antes de entregar fondos. Los bancos deben supervisar los nombres de las partes contenidas en estos mensajes y comparar los nombres con las listas de la OFAC. Consulte la sección del esquema general principal, "Oficina de Control de Activos Extranjeros", en las páginas 165 a 175, como guía. Los bancos con un gran volumen de mensajes de SWIFT deben determinar si sus actividades de supervisión son adecuados para detectar actividades sospechosas, especialmente si el mecanismo de supervisión no es automatizado. Consulte la sección del esquema general principal "Informes de actividades sospechosas", en las páginas 73 a 89, y la sección del esquema general ampliado "Transferencias de Fondos", en las páginas 237 a 244, como guía.

Las políticas, los procedimientos y los procesos deben, asimismo, exigir un control exhaustivo de toda la documentación aplicable a la actividad de financiación de comercio internacional (por ejemplo, declaraciones aduaneras, documentos del comercio internacional, facturas, etc.), para que el banco sea capaz de supervisar e informar acerca de actividades poco habituales o sospechosas, en función del papel que desempeña en el proceso relacionado con la carta de crédito. La sofisticación del proceso de control de la documentación y los sistemas para la información de gestión (MIS) deben ser acordes al tamaño y la complejidad de la cartera de financiación del comercio internacional del banco y su papel en el proceso relacionado con la carta de crédito. Además de los filtros de la OFAC, el proceso de supervisión debe permitir un escrutinio mayor de:

- Envíos de artículos que no se correspondan con el carácter del negocio del cliente (p. ej., una compañía siderúrgica que comienza a comerciar productos de papel, o una compañía de tecnología de información que comienza a comerciar productos farmacéuticos en grandes cantidades.
- Clientes que realicen negocios en jurisdicciones de mayor riesgo.
- Clientes que envíen artículos a través de jurisdicciones de mayor riesgo, incluido el tránsito por países no cooperantes.
- Clientes que participen en actividades de mayor riesgo potencial, incluidas las actividades que puedan están sujetas a restricciones de importación y exportación (p. ej., equipo para organizaciones policiales o militares de gobiernos extranjeros, armas, municiones, mezclas químicas, artículos clasificados de defensa, información técnica confidencial, materiales nucleares, piedras preciosas o determinados recursos naturales tales como metales, mineral metalífero y petróleo crudo).
- Evidente fijación irregular de precios en bienes y servicios.
- Tergiversación evidente de la cantidad o el tipo de bienes importados o exportados.
- El fraccionamiento de las transacciones que parezca innecesariamente complejo y diseñado para disimular el verdadero carácter de la transacción.
- Los casos en los cuales los clientes efectúen pagos de lo recaudado a un tercero no relacionado.

- Ubicaciones de envío o descripciones de bienes que no sean consistentes con la carta de crédito.

- Cartas de crédito significativamente enmendadas sin una justificación razonable o cambios de beneficiario o ubicación de pago. Cualquier cambio en los nombres de las partes debe promover un control adicional de la OFAC.

El 18 de Febrero de 2010, la FinCEN publicó una carta informativa a fin de instruir y asistir a la industria financiera con respecto a la presentación de informes sobre presuntos casos de lavado de dinero a través de transacciones. Este documento comprende ejemplos de "señales de advertencia" en función de las actividades reportadas en los SAR, que tanto la FinCEN como las autoridades a cargo del orden público consideran podrían indicar lavado de dinero a través de transacciones. A fin de colaborar con las autoridades de aplicación de la ley en su esfuerzo por detectar las actividades de lavado de dinero a través de transacciones (TBML) y cambio de "pesos" en el mercado negro (BMPE), en la carta informativa, la FinCEN solicita a las instituciones financieras que marquen la casilla correspondiente en la sección Información sobre actividades sospechosas del formulario SAR e incluyan la abreviación TBML o BMPE en la sección de descripción de dicho formulario. La carta informativa está disponible en www.fincen.gov.

A menos que el comportamiento del cliente o la documentación de la transacción sean poco habitual, no se debe exigir que el banco dedique tiempo o esfuerzo indebido controlando toda la información. Los ejemplos anteriores, especialmente en lo relativo al Banco emisor, pueden estar incluidos como parte de su proceso de CDD de rutina. Los bancos con programas de CDD sólidos, pueden llegar a la conclusión de que las transacciones individuales requieren un menor control, como resultado del conocimiento exhaustivo que tiene el banco de las actividades del cliente.

Procedimientos de Inspección

Actividades de financiación del comercio internacional

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de financiación del comercio internacional y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las actividades de financiación del comercio internacional. Evalúe la aptitud de las políticas, los procedimientos y los procesos que rigen las actividades relacionadas con la financiación del comercio internacional y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Evalúe la aptitud de la información de debida diligencia que el banco obtiene para los archivos del cliente. Determine si el banco dispone de procesos para obtener información al momento de la apertura de la cuenta, además de garantizar que se mantenga la información actualizada del cliente.

3. A partir de un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz la cartera de financiación del comercio internacional para detectar actividades sospechosas o poco habituales, particularmente aquellas que impongan un mayor riesgo de lavado de dinero.

4. Determine si el sistema del banco para supervisar las actividades de financiación del comercio internacional, detectar e informar sobre actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

5. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

6. En función del análisis de riesgos del banco de su cartera de financiación del comercio internacional, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de financiación del comercio internacional. A partir de la muestra seleccionada, revise la documentación de debida diligencia de los clientes para determinar si la información es acorde al riesgo del cliente. Identifique cualquier actividad sospechosa o poco habitual.

7. Verifique si el banco supervisa la cartera de financiación del comercio internacional para detectar tanto posibles violaciones a la OFAC como patrones de transacciones poco habituales, y si registra los resultados de cualquier tipo de debida diligencia.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las actividades de financiación del comercio internacional.

Banca Privada: Esquema General

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de banca privada y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia. Esta sección amplía la revisión principal de las exigencias normativas y legales de la banca privada para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

Las actividades de la banca privada se definen generalmente como aquellas en que se prestan servicios personalizados a clientes de mayor valor neto (p. ej., planificación del patrimonio, asesoría financiera, préstamos, administración de inversiones, pago de facturas, remisión de correo y mantenimiento de una residencia). La banca privada se ha convertido en un rubro de actividad comercial cada vez más importante para organizaciones bancarias importantes y diversas, así como una mejor fuente de ingresos de honorarios .

Los bancos estadounidenses pueden gestionar las relaciones asociadas con la banca privada, tanto para clientes nacionales como internacionales. Por lo general, los umbrales de servicio de banca privada se basan en la cantidad de activos que se gestionan y en la necesidad de productos o servicios específicos (p. ej., administración de bienes inmuebles, supervisión detallada de empresas, administración de dinero). Los honorarios que se cobran normalmente dependen del umbral de los activos, y del uso de productos y servicios específicos.

Las estrategias de banca privada por lo general se estructuran con un punto de contacto central (es decir, el gerente de relaciones) que actúa de enlace entre el cliente y el banco, y facilita la utilización por parte del cliente de los servicios y productos financieros del banco. El Apéndice N (“Banca privada: estructura común”) proporciona un ejemplo de una estructura típica de banca privada e ilustra la relación entre el cliente y el gerente de relaciones. Los productos y servicios típicos de la relación asociada con la banca privada incluyen los siguientes:

- Administración de dinero en efectivo (p. ej., cuentas corrientes, privilegio de giro en descubierto, barridos de efectivo y servicios de pago de facturas).
- Transferencias de fondos.
- Gestión de activos (p. ej., fideicomisos, asesoría sobre inversiones, administración de inversiones y servicios de custodia e intermediación).[222]

[222] Como guía, consulte el esquema general ampliado y procedimientos de inspección, “Servicios fiduciarios y de gestión de activos”, en las páginas 318 a 322 y 323 a 324, respectivamente.

- Facilitación de entidades instaladas en el exterior y compañías fantasma (p. ej., Compañías de inversión privada [PIC], corporaciones comerciales internacionales [IBC] y fideicomisos).[223]
- Servicios de préstamos (p. ej., hipotecarios, vía tarjetas de crédito, personales, vía cartas de crédito).
- Servicios de planificación financiera incluida la planificación tributaria y patrimonial.
- Servicios de custodia.
- Otros servicios según se requieran (p. ej., servicios de correo).

La privacidad y confidencialidad son elementos importantes en las relaciones asociadas con la banca privada. Aunque los clientes pueden elegir los servicios de banca privada simplemente para gestionar sus activos, puede suceder que también busquen un refugio confidencial, seguro y legítimo para su capital. Cuando actúan como fiduciarios, los bancos tienen obligaciones legales, contractuales y éticas que mantener.

Factores de riesgo

Los servicios de banca privada pueden ser vulnerables a las estratagemas de lavado de dinero y en el pasado los procesos judiciales por lavado de dinero han demostrado esa susceptibilidad. En *Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities* (Banca privada y lavado de dinero: estudio de caso sobre oportunidades y susceptibilidades)[224], del Subcomité Permanente de Investigaciones de 1999, se describieron parcialmente las siguientes susceptibilidades con respecto al lavado de dinero:

- Banqueros privados actuando como defensores de los clientes.
- Clientes poderosos, incluyendo personalidades sujetas a exposición política, industriales y artistas.
- Cultura de confidencialidad y la utilización de jurisdicciones donde se aplica el secreto o compañías fantasma.[225]
- Cultura de banca privada con controles internos laxos.
- Carácter competitivo del negocio.
- Potencial de beneficios significativos para el banco.

---

[223] Como guía, consulte el esquema general ampliado y procedimientos de inspección, "Entidades comerciales (nacionales y extranjeras)", en las páginas 357 a 363 y 364 a 365, respectivamente.

[224] Consulte frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_hearings&docid=f:61699.pdf.

[225] Consulte la sección del esquema general ampliado, "Entidades comerciales (nacionales y extranjeras)", en las páginas 357 a 363, como guía.

Mitigación del riesgo

Contar con políticas, procedimientos y procesos eficaces puede ayudar a los bancos a no convertirse en medios o víctimas del lavado de dinero, la financiación del terrorismo y otros delitos financieros que se cometen a través de las relaciones asociadas con la banca privada. La sección del esquema general principal "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", de la páginas 145 a 150, contiene información adicional relacionada con el análisis de riesgos y la debida diligencia. En último término, las actividades ilícitas realizadas a través de la unidad de banca privada pueden ocasionar costos financieros altos y riesgos que pueden afectar la reputación del banco. El impacto financiero puede incluir sanciones y multas regulatorias, gastos ocasionados por litigios, pérdida de negocios, reducción en la liquidez, confiscaciones y congelamiento de activos, pérdida de préstamos y gastos de reparaciones.

Análisis de riesgos de clientes

Los bancos deben analizar los riesgos que plantean sus actividades de banca privada en función del campo de aplicación de las operaciones y la complejidad las relaciones con sus clientes. La gerencia debe establecer un perfil de riesgo de cada cliente, que servirá para fijar prioridades en los recursos de supervisión y para la supervisión continua de las actividades de la relación. Se deben tomar en cuenta los siguientes factores al identificar las características del riesgo de los clientes de la banca privada:

- **Origen de la riqueza y carácter del negocio del cliente.** La fuente de la riqueza del cliente, el carácter del negocio del cliente y el grado en que sus antecedentes comerciales plantean un mayor riesgo de lavado de dinero y financiamiento del terrorismo. Estos factores deben tenerse en cuenta para las cuentas de banca privada abiertas para personalidades sujetas a exposición política (PEP).[226]

- **Propósito y actividad prevista.** El tamaño, el propósito, los tipos de cuentas, los productos y los servicios involucrados en la relación, y la actividad prevista de la cuenta.

- **Relación.** El carácter y duración de la relación del banco (incluidas las relaciones con las filiales) con el cliente de banca privada.

- **Estructura corporativa del cliente.** Tipo de estructura corporativa (p. ej., IBC, compañías fantasmas [nacionales o internacionales] o PIC).

- **Jurisdicción y ubicación geográfica.** Ubicación geográfica del domicilio del cliente de banca privada y de su negocio (nacional o internacional). En el control se debe tener en cuenta el grado en que la respectiva jurisdicción es reconocida internacionalmente por presentar un mayor riesgo de lavado de dinero o, por el contrario, por contar con normas AML firmes.

[226] Consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150; y la sección del esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333, como guía.

- **Información pública.** Información conocida o razonablemente disponible al banco acerca del cliente de banca privada. El campo de aplicación y la profundidad de este control deben depender del carácter de la relación y de los riesgos planteados.

Debida diligencia de los clientes

La CDD es fundamental al momento de establecer cualquier relación con ellos, y es vital respecto a los clientes de la banca privada.[227] Los bancos deben tomar medidas razonables para establecer la identidad de sus clientes de la banca privada y, según sea pertinente, de los usufructuarios de las cuentas. La debida diligencia adecuada variará según los factores de riesgo identificados anteriormente. Las políticas, los procedimientos y los procesos deben definir la CDD aceptable para los distintos tipos de productos (p. ej., PIC), servicios y titulares de la cuenta. Como la debida diligencia es un proceso continuo, un banco debe tomar medidas para garantizar que los perfiles de cuenta sean actuales y la supervisión se establezca en función del riesgo. Los bancos deben tener en cuenta si los perfiles de riesgo deben ajustarse o la actividad sospechosa debe informarse cuando ésta no sea coherente con el perfil.

En relación con el CIP, no se exige que el banco revise las cuentas de banca privada para verificar la identidad de los beneficiarios; por el contrario, sólo se exige que verifique la identidad del titular de la cuenta designado. No obstante, la reglamentación del CIP también determina que, en función del análisis de riesgos del banco de una nueva cuenta abierta por un cliente que no es una persona física (p. ej., cuentas de la banca privada abiertas para una PIC), es posible que el banco deba "obtener información sobre" las personas físicas con autoridad o control sobre dicha cuenta, incluidos los firmantes, para verificar la identidad del cliente[228] y determinar si la cuenta se mantiene para ciudadanos no estadounidenses.[229]

Antes de abrir cuentas, los bancos deben recopilar la siguiente información de los clientes de la banca privada:

- Propósito de la cuenta.
- Tipo de productos y servicios que se usarán.
- Actividad prevista de la cuenta.
- Descripción y antecedentes de la fuente de la riqueza del cliente.

---

[227] La sección 312 de la Ley PATRIOTA de los EE. UU. exige que se establezcan políticas, procedimientos y procesos de debida diligencia de las cuentas de banca privada para ciudadanos no estadounidenses. Consulte la sección del esquema general principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 145 a 150, como guía.

[228] 31 CFR 103.121(b)(2)(ii)(C).

[229] Consulte los procedimientos de inspección de la sección principal, "Programa de debida diligencia de la banca privada (ciudadanos no estadounidenses)", en las páginas 151 a 153, como guía.

- El valor estimado del patrimonio neto del cliente, incluidos los estados financieros.
- La fuente actual de los fondos de la cuenta.
- Referencias u otra información para confirmar la reputación del cliente.

Acciones al portador

Algunas compañías fantasmas expiden acciones al portador (es decir, se concede la propiedad a través de acciones al portador, lo que permite que se transfiera la propiedad de la corporación simplemente mediante la transferencia de la posesión física de las acciones). Para mitigar el riesgo, las compañías fantasmas que expiden acciones al portador pueden, por ejemplo, mantener el control de las acciones al portador, encomendar las acciones a un tercero independiente confiable o exigir una certificación periódica de la propiedad. Los bancos deben analizar los riesgos que estas relaciones plantean y determinar los controles adecuados. Por ejemplo, en la mayoría de los casos los bancos deberían optar por mantener (o solicitar a un tercero que mantenga) las acciones al portador de los clientes. En algunos casos poco frecuentes que implican un riesgo menor, es posible que a los bancos les resulte eficaz recertificar periódicamente el usufructo de los clientes conocidos o antiguos. Un firme programa de CDD consiste en un control subyacente eficaz a través del cual los bancos pueden determinar el carácter, el propósito y el uso previsto de las compañías fantasmas, y aplicar normas adecuadas en cuanto a la documentación y supervisión.

Supervisión de la junta directiva y la alta gerencia

La supervisión activa de la junta directiva y la alta gerencia de las actividades de banca privada y la creación de una cultura de supervisión corporativa adecuada son elementos esenciales de una gestión de riesgos y un entorno de control responsables. El propósito y los objetivos de las actividades de banca privada de la organización deben ser identificados y comunicados claramente por la junta y la alta gerencia. Objetivos y metas bien desarrollados deben describir el tipo de clientela en términos de valor neto mínimo, activos invertibles y tipos de productos y servicios que se solicitan. Asimismo, deben también delimitar específicamente los tipos de clientes que el banco aceptará y no aceptará y deben establecer los niveles de autorización adecuados para la aceptación de nuevos clientes. La junta y la alta gerencia también deben participar activamente en el establecimiento de metas de control y gestión de riesgos de las actividades de banca privada, incluidos controles eficaces de auditoría y cumplimiento. Cada banco debe garantizar que sus políticas, procedimientos y procesos para llevar a cabo actividades de banca privada se evalúen y actualicen regularmente, así como también que se delineen claramente los papeles y las responsabilidades.

Los planes de compensación de empleados a menudo se basan en la cantidad de nuevas cuentas establecidas o en el aumento de los activos gestionados. La junta y la alta gerencia deben garantizar que los planes de compensación no incentiven a los empleados a ignorar los procedimientos de debida diligencia y apertura de cuentas adecuados o las posibles actividades sospechosas relacionadas con la cuenta. Los procedimientos que exigen diversos niveles de aprobación para aceptar nuevas cuentas de banca privada pueden minimizar dichas posibilidades.

Dado el carácter delicado de la banca privada y la responsabilidad potencial asociada con ella, los bancos deben investigar exhaustivamente los antecedentes de los gerentes de relaciones asociadas con la banca privada recién contratados. Durante el período de empleo, cualquier indicio de actividad inadecuada debe ser investigado prontamente por el banco.

Además, cuando los gerentes de relaciones asociadas con la banca privada cambian de empleador, a menudo sus clientes se van con ellos. Los bancos tienen la misma responsabilidad potencial respecto a los clientes existentes de funcionarios recién contratados como respecto a cualquier relación nueva asociada con la banca privada. Por lo tanto, dichas cuentas deben revisarse sin demora, utilizando los procedimientos del banco para establecer nuevas relaciones asociadas con las cuentas.

Los sistemas para la información de gestión (MIS) y sus informes también son importantes para supervisar y gestionar de manera eficaz los riesgos y las relaciones asociadas con la banca privada. La junta y la alta gerencia deben controlar los informes de compensación del gerente de relaciones, los informes de comparación de objetivo o presupuesto y los informes de gestión de riesgos aplicables. Los informes de MIS de banqueros privados deben permitir al gerente de relaciones ver y gestionar la totalidad de la relaciones con el cliente y cualquier otra relacionada.

Procedimientos de Inspección

Banca privada

Objetivo: *Evaluar la aptitud de los sistemas del banco para gestionar los riesgos asociados con las actividades de banca privada y la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia. Esta sección amplía la revisión principal de las exigencias normativas y legales de la banca privada para proporcionar un análisis más minucioso de los riesgos AML asociados a esta actividad.*

1. Revise las políticas, los procedimientos y los procesos con respecto a las actividades de banca privada. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de banca privada del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. A partir de un control de los informes de los MIS (p. ej., informes sobre acumulación de los clientes, excepciones a las políticas y documentación faltante, clasificación de riesgos de clientes, actividad poco habitual de cuentas y concentración de clientes) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con la banca privada, particularmente aquellas que planteen un alto riesgo de lavado de dinero.

3. Determine si el sistema del banco para supervisar las relaciones asociadas con la banca privada, detectar e informar sobre actividades sospechosas, es adecuado a su tamaño, complejidad, ubicación y los tipos de relaciones que mantiene con los clientes.

4. Revise el programa de compensación de la banca privada. Determine si incluye medidas cualitativas que se proporcionen a los empleados para cumplir con las exigencias de supervisión y elaboración de informes de actividades sospechosas y apertura de cuentas.

5. Revise el programa de supervisión que el banco utiliza para examinar la condición financiera personal del gerente de relaciones de la banca privada y para detectar cualquier actividad inapropiada.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, “Oficina de Control de Activos Extranjeros”, en las páginas 176 a 178, como guía.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus actividades de banca privada, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de cuentas de banca privada. La muestra debe incluir los siguientes tipos de cuentas:

   - Personalidades sujetas a exposición política (PEP).

- Compañías de inversión privada (PIC), corporaciones comerciales internacionales (IBC) y compañías fantasmas.
- Entidades instaladas en el exterior.
- Negocios que manejan un alto flujo de efectivo.
- Compañías importadoras y exportadoras.
- Clientes que realizan negocios en una ubicación geográfica de mayor riesgo o que provienen de dicha ubicación geográfica.
- Clientes incluidos en informes de supervisión de actividades poco habituales.
- Clientes que efectúan transacciones de grandes volúmenes en dólares y transferencias de fondos frecuentes.

8. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:
   - Revise la documentación de apertura de la cuenta e información de debida diligencia continua.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones.
   - Compare las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el tipo de negocio del cliente.
   - Identifique cualquier actividad sospechosa o poco habitual.
9. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos con respecto a las relaciones asociadas con la banca privada.

Servicios Fiduciarios y de Gestión de Activos: Esquema General

Objetivo: *Evaluar la aptitud de las políticas, los procedimientos y los procesos del banco, y los sistemas para gestionar los riesgos asociados con los servicios fiduciarios y de gestión de activos,[230] así como la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Las cuentas fiduciarias[231] generalmente se definen como un acuerdo legal en el cual una parte (el fideicomitente u otorgante) transfiere la propiedad de los activos a una persona o banco (el fiduciario) para que lo conserve o utilice en beneficio de terceros. Estos acuerdos incluyen las categorías amplias de cuentas supervisadas por tribunales (p. ej., albaceazgo o custodias), fideicomisos personales (p. ej., fideicomisos establecidos en vida, fideicomisos testamentarios y fideicomiso benéfico), y los fideicomisos corporativos (p. ej., administración fiduciaria de bonos).

A diferencia de los acuerdos fiduciarios, las cuentas de agencia se establecen por contrato y se rigen por el derecho contractual. Los activos están sujetos a los términos del contrato y el título o la propiedad no se transfieren al banco en calidad de agente. Las cuentas de agencia incluyen las relaciones de custodia, plica, administración de inversiones,[232] y que impliquen cajas de seguridad. Los productos y servicios agenciados pueden ofrecerse en un departamento fiduciario tradicional o a través de otros departamentos del banco.

Programa de identificación de clientes

Las normas del CIP, vigentes a partir del 1.º de Octubre de 2003, son aplicables básicamente a todas las cuentas bancarias abiertas después de esa fecha. La definición de "cuenta" establecida en la norma CIP incluye las relaciones de administración de efectivo, de custodia, fiduciarias y que impliquen cajas de seguridad. Sin embargo, la norma CIP excluye las cuentas de beneficios sociales de empleados establecidas conforme a la Ley de Seguridad de los Ingresos para el Retiro de los Empleados de 1974 (ERISA, por sus siglas en inglés).

---

[230] Las cuentas de administración de activos pueden ser cuentas fiduciarias o de agencia, y son gestionadas por el banco.

[231] La Oficina del Interventor Monetario y la Oficina de Supervisión de Instituciones de Ahorro utilizan el término más amplio "relación de carácter fiduciario" en vez de "fideicomiso". En la relación de carácter fiduciario intervienen un fiduciario, un albacea, un administrador, un registrador de acciones y bonos, un agente de transferencia, un depositario, cesionario, un receptor o un curador actuando bajo la ley uniforme de donaciones a menores; un asesor de inversiones, si el banco recibe honorarios por su asesoría sobre inversiones; y cualquier relación bajo la cual el banco posea la capacidad de decidir discrecionalmente sobre inversiones en nombre de otro (12 CFR 9-2(e) y 12 CFR 550.30).

[232] Para los propósitos de los bancos nacionales y las asociaciones de ahorro reguladas por la Oficina de Supervisión de Instituciones de Ahorro, ciertas actividades de administración de inversiones, como proporcionar asesoría de inversión a cambio de honorarios, son de naturaleza "fiduciaria".

A los efectos del CIP, no se exige que un banco revise las cuentas fiduciarias, de depósito en plica o similares para verificar la identidad de los beneficiarios, en cambio, sólo debe verificar la identidad del titular de la cuenta designado (el fideicomiso). En el caso de las cuentas fiduciarias, el cliente es el fideicomiso, sea o no el banco el fiduciario en el fideicomiso. Sin embargo, la norma CIP también estipula que, en función del análisis realizado por el banco del riesgo que implica una cuenta nueva abierta por un cliente que no es persona física, el banco deberá "obtener información acerca" de las personas que tienen el control o la autoridad sobre la cuenta, incluidos los firmantes, para verificar la identidad del cliente.[233] Por ejemplo, en ciertas circunstancias relativas a fideicomisos revocables, el banco deberá obtener información sobre el constituyente, otorgante, fideicomitente u otras personas con autoridad para dar órdenes al fiduciario, y que por lo tanto tienen autoridad o control sobre la cuenta, para establecer la verdadera identidad del cliente.

En el caso de las cuentas de depósito en plica, si un banco abre una cuenta a nombre de un tercero, como un agente inmobiliario, que actúa como agente de depósito en plica, entonces el cliente del banco es el agente de depósito en plica. Si el banco es el agente de depósito en plica, entonces la persona que establece la cuenta es el cliente del banco. Por ejemplo, si un comprador de bienes inmuebles abre directamente una cuenta de depósito en plica y deposita fondos a ser pagados al vendedor una vez satisfechas ciertas condiciones específicas, el cliente del banco será el comprador. Además, si una compañía en formación establece una cuenta de depósito en plica para que los inversionistas depositen sus aportes mientras está pendiente el monto mínimo requerido, el cliente del banco será la compañía en formación (o si aún no tiene personalidad jurídica, la persona que abre la cuenta en su nombre). Sin embargo, la norma CIP también estipula que, en función del análisis de riesgo realizado por el banco de una nueva cuenta abierta por un cliente que no es persona física, es posible que el banco deba "obtener información acerca" de las personas que tienen autoridad o control sobre dicha cuenta, incluidos los firmantes, para verificar la identidad del cliente.[234]

Factores de riesgo

Las cuentas de gestión fiduciaria y de activos, incluidas las relaciones con agencias, presentan riesgos relativos a BSA/AML similares a los que presenta el recibo de depósitos, los préstamos y otras actividades bancarias tradicionales. Las preocupaciones se deben principalmente a las estructuras de relación únicas que se presentan cuando los bancos manejan actividades fiduciarias y agenciadas, como las siguientes:

- Cuentas personales y cuentas supervisadas por tribunales.
- Cuentas fiduciarias generadas en el departamento de banca privada.
- Cuentas de administración de activos y asesoría sobre inversiones.

---

[233] Consulte 31 CFR 103.121(b)(2)(ii)(C).

[234] Id.

- Cuentas nacionales y mundiales de custodia.
- Préstamos en valores.
- Cuentas de beneficios sociales y de retiro de empleados.
- Cuentas fiduciarias corporativas.
- Cuentas de agentes de transferencia.
- Otros rubros de actividad comercial relacionados.

Como en cualquier otra relación de cuenta, el riesgo de lavado de dinero puede presentarse en las actividades de gestión fiduciaria y de activos. Cuando existe uso indebido de las cuentas de gestión fiduciaria y de activos, se puede ocultar el origen y el uso de los fondos, así como la identidad de los usufructuarios y propietarios legales. Los clientes y usufructuarios de las cuentas pueden tratar de permanecer anónimos para transferir fondos ilícitos o evitar escrutinios. Por ejemplo, los clientes pueden buscar cierto nivel de anonimato creando Compañías de inversión privada (PIC),[235] fideicomisos en el exterior u otras entidades de inversión que oculten la propiedad real o el derecho de usufructo del fideicomiso.

Mitigación del riesgo

La gerencia debe establecer políticas, procedimientos y procesos que le permitan al banco identificar relaciones y circunstancias de cuentas poco habituales, activos y origen de activos cuestionables y otras áreas potenciales de riesgo (p. ej., cuentas en el exterior, PIC, planes de protección patrimonial en el extranjero (APT, por sus siglas en inglés),[236] cuentas de agencia y beneficiarios no identificados). A pesar de que la mayoría de cuentas de gestión fiduciaria y de activos tradicionales no necesitarán una EDD, la gerencia debe estar alerta respecto a aquellas situaciones que requieran control o investigación adicional.

Comparación de los clientes con las listas

El banco debe conservar la información del CIP exigida y realizar la comparación por única vez de los nombres de las cuentas fiduciarias con las solicitudes de búsqueda de la sección 314(a). El banco también debe poder identificar a los clientes que puedan ser personalidades sujetas a exposición política (PEP), que negocien o se localicen en jurisdicciones designadas como “de interés principal con respecto al lavado de dinero”

[235] Consulte la sección del esquema general ampliado, “Entidades comerciales (nacionales y extranjeras)”, en las páginas 357 a 363, para obtener orientación adicional sobre las PIC.

[236] Las APT son una forma especial de fideicomiso irrevocable, por lo general creadas (establecidas) fuera del país con el fin principal de preservar y proteger una parte de la riqueza de una persona contra los acreedores. La titularidad del activo se transfiere a una persona denominada el fiduciario. Las APT por lo general son neutrales tributariamente y su función última es la de brindar sustento a los beneficiarios.

bajo la sección 311 de la Ley PATRIOTA de los EE. UU. o que concuerden con las listas de la OFAC.[237] Como práctica responsable, el banco también debe determinar la identidad de las demás partes que puedan tener control sobre la cuenta, como los otorgantes fiduciarios conjuntos. Consulte la sección del esquema general principal, "Intercambio de información", en las páginas 108 a 114, y la sección del esquema general ampliado, "Personalidades sujetas a exposición política", en las páginas 329 a 333, como guía.

Circunstancias que requieren una debida diligencia especial

La gerencia debe analizar el riesgo de una cuenta en función de una variedad de factores, que pueden incluir:

- El tipo de cuenta de agencia o fiduciaria y su tamaño.
- Los tipos y la frecuencia de las transacciones.
- El país de residencia de los titulares o beneficiarios, o el país en el que se establecieron, o la fuente de los fondos.
- Las cuentas y transacciones que no sean habituales o acostumbradas para el cliente o el banco.
- Deben establecerse procedimientos estrictos de documentación, verificación y supervisión de transacciones para las cuentas que la gerencia considere de mayor riesgo. Generalmente, las cuentas de beneficios sociales de los empleados y las cuentas supervisadas por tribunales están entre las de más bajo riesgo BSA/AML.

Los siguientes constituyen ejemplos de situaciones en las cuales posiblemente sea adecuado llevar a cabo la debida diligencia especial:

- Al iniciar el banco una relación con un cliente nuevo.
- Los usufructuarios o beneficiarios de la cuenta residen en una jurisdicción extranjera, o el fideicomiso o sus mecanismos de obtención de fondos están establecidos en el exterior.
- Los activos o las transacciones son inusuales para el tipo y carácter de cliente.
- El tipo de cuenta, el tamaño, los activos o las transacciones son atípicas para el banco.

---

[237] La gerencia y los inspectores deben ser conscientes de que la comparación con las listas de la OFAC no es una exigencia de la BSA. Sin embargo, dado que los sistemas fiduciarios generalmente son diferentes a los sistemas bancarios y están separados de los mismos, esta verificación en el sistema bancario no basta para garantizar que también se lleven a cabo en el departamento de gestión fiduciaria y administración de activos. Por otra parte, la posición de la OFAC es que el beneficiario de una cuenta tiene intereses contingentes o futuros en los fondos de la cuenta y, de manera coherente con el perfil de riesgo del banco, se debe realizar una revisión de los beneficiarios para asegurar el cumplimiento OFAC. Consulte la sección del esquema general principal, "Oficina de Control de Activos Extranjeros", en las páginas 165 a 175, como guía.

- Las transferencias de fondos internacionales se realizan particularmente a través de fuentes de fondos ubicadas en el exterior.
- Las cuentas se financian con activos fácilmente trasladables, como piedras preciosas, metales preciosos, monedas, obras de arte, estampillas poco comunes o instrumentos negociables.
- Se mantienen cuentas o relaciones en las que la identidad de los usufructuarios o beneficiarios o la fuente de los fondos son desconocidos o no se pueden establecer con facilidad.
- Las cuentas benefician a entidades de beneficencia u otras organizaciones no gubernamentales (ONG) que pueden ser utilizadas como conducto para realizar actividades ilegales.[238]
- Cuentas fiduciarias de abogados con rendimiento de interés (IOLTA) que mantienen y procesan montos significativos en dólares.
- Activos de las cuentas que incluyen PIC.
- En las cuentas o transacciones son parte personalidades sujetas a exposición política (PEP).

[238] Como guía adicional, consulte la sección del esquema general ampliado, "Organizaciones no gubernamentales y entidades de beneficencia", en las páginas 353 y 354.

Procedimientos de Inspección

Servicios de gestión de fideicomisos y de activos

Objetivo: *Evaluar la aptitud de las políticas, los procedimientos y los procesos del banco, y los sistemas para gestionar los riesgos asociados con los servicios fiduciarios y de gestión de activos,[239] así como la capacidad de la gerencia de implementar sistemas eficaces de supervisión, informe y debida diligencia.*

Si esta es una inspección de fideicomisos independiente, consulte los procedimientos de inspección de la sección principal "Campo de aplicación y planificación", en las páginas 20 a 22, como guía exhaustiva del campo de aplicación de la inspección BSA/AML. En ese caso, la inspección puede necesitar cubrir áreas adicionales, que incluyen la capacitación, el funcionario de cumplimiento de la BSA, el control independiente y los elementos de seguimiento.

1. Revise las políticas, los procedimientos y los procesos con respecto a los servicios de gestión de fideicomisos y de activos. Evalúe la aptitud de las políticas, los procedimientos y los procesos en relación con las actividades de servicios de gestión de fideicomisos y de activos del banco y los riesgos que éstas plantean. Analice si los controles son adecuados para proteger razonablemente al banco del lavado de dinero y el financiamiento del terrorismo.

2. Revise los procedimientos del banco para reunir la información de identificación adicional, cuando sea necesario, sobre el constituyente, el otorgante, el fiduciario, u otras personas con autoridad para instruir al fiduciario, y que por lo tanto ejerzan autoridad o control sobre la cuenta, con el objetivo de establecer la verdadera identidad del cliente.

3. De un control de los sistemas para la información de gestión (MIS) y los factores de valoración de riesgos internos, determine si el banco identifica y supervisa de manera eficaz las relaciones asociadas con la gestión de activos y fideicomisos, particularmente aquellas que planteen un mayor riesgo de lavado de dinero.

4. Determine si el banco incluye las relaciones de gestión de fideicomisos y de activos en todo el banco o, según corresponda, en los sistemas de acumulación BSA/AML de toda la institución.

5. Determine si el sistema del banco para supervisar las relaciones asociadas con la gestión de fideicomisos y de activos, detectar e informar actividades sospechosas, es adecuado dados el tamaño, la complejidad, la ubicación y los tipos de relaciones con los clientes del banco.

6. Si corresponde, consulte los procedimientos de inspección de la sección principal, "Oficina de Control de Activos Extranjeros", en las páginas 176 a 178, como guía.

---

[239] Las cuentas de administración de activos pueden ser cuentas fiduciarias o de agencia, y son gestionadas por el banco.

Pruebas de transacciones

7. En función del análisis de riesgos del banco de sus relaciones con la gestión de fideicomisos y de activos, como también de informes de inspecciones previas y de auditoría, seleccione una muestra de las relaciones con los servicios de gestión de fideicomisos y de activos de mayor riesgo. Incluya las relaciones con los otorgantes y los fiduciarios conjuntos, si tienen autoridad o control, así como los activos de mayor riesgo como las Compañías de inversión privada (PIC) o los planes de protección patrimonial en el extranjero. De la muestra seleccionada, lleve a cabo los siguientes procedimientos de inspección:

   - Revise la documentación de apertura de la cuenta, incluidos los CIP, para asegurarse de que se haya llevado a cabo la debida diligencia adecuada y mantenido los registros adecuados.
   - Revise los estados de cuenta y, según sea necesario, detalles específicos de las transacciones. Compare las transacciones previstas con la actividad real.
   - Determine si la actividad real es coherente con el tipo de negocio del cliente y el propósito declarado de la cuenta.
   - Identifique cualquier actividad sospechosa o poco habitual.

8. En función de los procedimientos de inspección realizados, incluidas las pruebas de transacciones, formule una conclusión sobre la aptitud de las políticas, los procedimientos y los procesos asociados con las relaciones de gestión de fideicomisos y de activos.