MANUAL DEL EXAMINADOR - INTRODUCCION

LEY DEL SECRETO BANCARIO Y LUCHA CONTRA EL LAVADO DE DINERO.

El 30 de junio del año 2005 el Departamento del Tesoro de los Estados Unidos (Financial Crimen Enforcement Network. United Status Department of Treasury) emitió el Bank Secrecy Act/Anti-Money Laundering Examination Manual, esfuerzo realizado con el fin de asegurar una adecuada aplicación de la Ley del Secreto Bancario (Bank Secrecy Act) por parte de las instituciones financieras.

FELABAN, consciente de la importancia y de los aportes que brinda este documento para la comunidad financiera en Latinoamérica, realizó una traducción libre para conocimiento y mejor comprensión de nuestros asociados de dicho documento.

El presente “Manual del Examinador. Ley del Secreto Bancario y Lucha contra el Lavado de Dinero”, no es oficial, constituye tan solo una guía; el documento oficial con sus respectivos apéndices, es el originalmente publicado por Financial Crimen Enforcement Network. United Status Department of Treasury que puede ser encontrado en la página: http://www.fincen.gov/bsaamlmanualnr.htm.

[logotipo del FFIEC]

Manual del Examinador

Ley del Secreto Bancario y Lucha contra el Lavado de Dinero

Junta de Gobernadores del Sistema de la Reserva Federal, Corporación Federal de Seguros de Depósitos *[Federal Deposit Insurance Corporation]*, Administración Nacional de Cooperativas de Crédito *[National Credit Union Administration]*, Oficina del Contralor de la Moneda *[Office of the Comptroller of the Currency]*, Oficina de Supervisión de Entidades de Ahorro y Crédito *[Office of Thrift Supervision]*.

Manual del Examinador

Ley del Secreto Bancario y Lucha contra el Lavado de Dinero

Junio de 2005

MANUAL DE EXAMINADORES -LEY DEL SECRETO BANCARIO Y LUCHA CONTRA EL LAVADO DE DINERO

Índice

Registros de cuentas de corresponsalía extranjeras y

debida diligencia Programa de debida diligencia de banca privada

(para quienes no son ciudadanos de EE. UU.) Medidas especiales

Informes sobre bancos extranjeros y cuentas financieras Informes sobre el transporte internacional de moneda o instrumentos

financieros

Oficina de Control de Activos Extranjeros (OFAC)

Conclusiones y finalización del examen

VISIÓN AMPLIADA DE LOS PROCEDIMIENTOS DE LOS EXÁMENES

Programa de cumplimiento BSA / AML empresarial integral 103

PRODUCTOS Y SERVICIOS Banca corresponsal (nacional y extranjera)

Cuentas de corresponsalía (nacionales)

Cuentas de corresponsalía (extranjeras)

Letras de cambio o libranzas en dólares de EE. UU. [US Dollar Drafts]

Cuentas usadas para pagos [Payable Through Accounts]

Actividades de transporte de valores bancarios [Pouch Activities]

Sucursales y oficinas extranjeras de bancos de EE. UU.

Banca paralela

Banca electrónica

Servicios de pagos electrónicos

Transferencia de fondos

Efectivo electrónico

Procesadores de pagos de terceros

Compraventa de instrumentos monetarios

Servicios para cuentas de depósito y no depósito

Depósitos a través de intermediarios o comisionistas

Cajeros automáticos de propiedad privada

Productos de inversión de no depósito

Seguros

Cuentas de concentración Actividades de préstamos Actividades de financiación comercial Banca privada Servicios de administración de fiducias y activos PERSONAS Y ENTIDADES Extranjeros no residentes y personas naturales extranjeras Personas expuestas políticamente Cuentas de embajadas y consulados extranjeros Entidades financieras no bancarias Proveedores de servicios profesionales Organizaciones no gubernamentales y entidades de beneficencia Corporaciones (nacionales y extranjeras) Negocios intensivos en capital

APÉNDICES Apéndice A – Legislación y reglamentación BSA [Ley del Secreto

Este Manual del Examinador de la Ley del Secreto Bancario (BSA por su sigla en inglés para Bank Secrecy Act) y la Lucha contra el Lavado de Dinero (AML por su sigla en inglés para Anti-Money Laundering) del Consejo de Exámenes de las Instituciones Financieras Federales (FFIEC) de Estados Unidos es una guía útil para los examinadores que ofrecen los exámenes del programa de cumplimiento con la BSA/AML y la Oficina de Control de Activos Extranjeros (OFAC por su sigla en inglés para Office of Foreign Assets Control). Un eficaz programa de cumplimiento con la Ley del Secreto Bancario y la Lucha contra el Lavado de Activos (BSA/AML) requiere una sólida gestión de riesgo, y por lo tanto el manual también es útil como guía para identificar y controlar los riesgos asociados al lavado de dinero y la financiación del terrorismo. El manual contiene una visión general de los requisitos del programa de cumplimiento BSA/AML, las expectativas con respecto a los riesgos y la gestión de riesgo que implican la BSA/AML, las buenas prácticas de la industria y los procedimientos empleados para los exámenes. El manual es el resultado del esfuerzo conjunto realizado por las agencias bancarias federales[1] y la Red de Control de Delitos Financieros (FinCEN, por su sigla en inglés para Financial Crimes Enforcement Network), una oficina del Departamento del Tesoro de los Estados Unidos, esfuerzo cuyo objetivo es la aplicación coherente de los requisitos de la BSA/AML. Por su parte, la OFAC colaboró con el desarrollo de los apartes del manual relativos a las revisiones de la OFAC. A manera de guía favor remitirse a los apéndices A ("Leyes y reglas BSA"), B ("Directivas BSA/AML") y C ("Referencias BSA/AML").

ESTRUCTURA DEL MANUAL

Para poder asignar recursos con efectividad y asegurar el cumplimiento de los requisitos de la Ley del Secreto Bancario, este manual se ha organizado de manera que los examinadores puedan adaptar el alcance y los procedimientos de los exámenes BSA/AML al perfil de riesgo específico de cada organización bancaria. El manual consta de las siguientes secciones:

. • Introducción
. • Núcleo [o aspectos fundamentales]: Generalidades y procedimientos
. • Ampliación: Generalidades y procedimientos
. • Apéndices

El núcleo y la visión general ampliada sirven de guía narrativa y presentan los antecedentes de cada tema; los procedimientos sirven de guía para el examinador. Las partes centrales o fundamentales [core sections] constituyen la plataforma de los

[1] Las cinco agencias bancarias federales que hacen parte del FFIEC son la Junta de Gobernadores del Sistema de la Reserva Federal, la Corporación Federal de Seguros de Depósitos [Federal Deposit Insurance Corporation], la Administración Nacional de Cooperativas de Crédito [National Credit Union Administration], la Oficina del Contralor de la Moneda [Office of the Comptroller of the Currency] y la Oficina de Supervisión de Entidades de Ahorro y Crédito [Office of Thrift Supervision].

exámenes BSA/AML [sobre la Ley del Secreto Bancario y la Lucha contra el Lavado de

Dinero] y en su mayoría, tratan aspectos jurídicos y los requisitos regulatorios del programa de cumplimiento BSA/AML. Las secciones de alcance y planificación le ayudan al examinador a preparar un plan de exámenes adecuado. En ocasiones aparece un mismo tema tanto en las secciones fundamentales como en las ampliadas (por ejemplo, transferencias de fondos y banca corresponsal extranjera). En esos casos las generalidades y los procedimientos de la sección fundamental tratan los requerimientos de la Ley del Secreto Bancario [BSA], mientras que las generalidades y procedimientos de la sección ampliada tratan los riesgos AML [relativos a la Lucha contra el Lavado de Dinero] que tiene la actividad específica.

Como mínimo, los examinadores deben emplear los procedimientos que se incluyen en las siguientes secciones básicas de este manual para asegurarse de que cada banco respectivo cuente con un programa adecuado de cumplimiento BSA/AML correspondiente a su propio perfil de riesgo:

. • Determinación del alcance y planeación (ver páginas 170 a 173)
. • Programa de cumplimiento BSA/AML (ver páginas 174 a 178)
. • Conclusiones y finalización del examen (ver páginas 210 a 213).

Si bien son separadas y distintas a las secciones BSA/AML, las partes fundamentales incluyen también generalidades y procedimientos válidos para examinar las políticas, procedimientos y procesos empleados por el banco para asegurar el cumplimiento de las sanciones OFAC [Oficina de Control de Activos Extranjeros]. El examinador debe revisar la evaluación de riesgo y la auditoria del banco según la OFAC para determinar el grado hasta el cual es necesario revisar el programa OFAC del banco durante el examen. Ver los procedimientos de la "Oficina de Control de Activos Extranjeros" en las páginas 207 a 209.

Las secciones ampliadas presentan líneas específicas de negocios, productos o entidades que pueden representar retos únicos y exposición [al riesgo] para los bancos. Ante ellas los bancos deben instituir políticas, procedimientos y procesos apropiados. De no estar presentes estos controles, estas líneas de negocios, productos o entidades podrían incrementar el riesgo BSA/AML. Además, en la sección ampliada se ofrece orientación sobre la gestión de riesgo empresarial integral BSA/AML.

No todos los procedimientos fundamentales y ampliados aplican a toda entidad bancaria. Los procedimientos concretos que será necesario aplicar dependen del perfil de riesgo BSA/AML de cada organización bancaria, la calidad y cantidad de pruebas independientes que existan, la historia de cumplimiento BSA/AML de la entidad financiera y otros factores relevantes.

ANTECEDENTES

En 1970 el Congreso de los Estados Unidos aprobó la Ley de Informes Monetarios y Transacciones en el Exterior [Currency and Foreign Transactions Reporting Act], más conocida como la "Ley del Secreto Bancario"[2] [BSA, por su sigla en inglés], la cual fijó

[2] 31 USC [Código de los Estados Unidos, por United States Code] 5311 *et seq*., 12 USC 1829(b) y 19511959. Ver también 12 USC 1818(s) (entidades de depósito [depositary institutions] con seguro federal) y 12 USC 1786 (q) (cooperativas de crédito [credit unions] con seguro federal).

requisitos al registro de datos y la elaboración de informes por personas naturales [private individuals], bancos[3] y otras entidades financieras. La BSA tenía como objetivo identificar la fuente, volumen y movimiento de moneda y otros instrumentos monetarios transportados o transmitidos hacia o desde los Estados Unidos o depositados en entidades financieras. La ley se propuso lograr este objetivo fijándole a las personas naturales, los bancos y otras entidades financieras la obligación de presentar informes sobre transacciones de dinero al Departamento del Tesoro de los Estados Unidos, identificar de manera adecuada a las personas que realizan dichas transacciones, y mantener un registro documental de las transacciones financieras. Dichos registros le permiten a las autoridades y entes reguladores adelantar investigaciones sobre posibles violaciones de tipo penal, fiscal o regulatorias, según corresponda, y sirven [además] como pruebas útiles en la persecución judicial del lavado de dinero y otros delitos financieros.

La Ley del Control al Lavado de Dinero de 1986 [Money Laundering Control Act] incrementó la efectividad de la Ley del Secreto Bancario [BSA] al relacionar las secciones 8(s) y 21 [de la misma] con la Ley de Seguros Federales para Depósitos [FDI -Federal Deposit Insurance Act], cuya secciones aplican por igual a todo banco de cualquier índole.[4] La Ley del Control al Lavado de Dinero de 1986 evita la posibilidad de que sean burlados los requisitos establecidos por la Ley del Secreto Bancario al fijarle responsabilidad penal a las personas naturales y entidades financieras que conscientemente colaboren con el lavado de dinero o estructuren sus transacciones para evitar la obligación de reportarlo. La Ley de 1986 le exigió a la banca fijar y mantener procedimientos razonables para asegurar y hacerle seguimiento al cumplimiento de los requisitos sobre registros que estableció la Ley del Secreto Bancario. Como consecuencia de ello, el 27 de enero de 1987 todas las agencias bancarias federales de Estados Unidos expidieron regulaciones básicamente similares, en las que se obliga a la banca a desarrollar programas de cumplimiento con los requisitos fijados por dicha Ley.

La Ley Annunzio-Wylie Contra el Lavado de Dinero de 1992 endureció las sanciones a las violaciones de la Ley del Secreto Bancario y fortaleció el papel del Departamento del Tesoro de los Estados Unidos. Dos años después, el Congreso de EE. UU. aprobó la Ley de Supresión del Lavado de Dinero de 1994 (MLSA, por su sigla en inglés), la cual también abordó el papel de dicho Departamento del Tesoro en la lucha contra el lavado de dinero.

En abril de 1996 se desarrolló el Reporte de operaciones sospechosas (ROS; en inglés SAR, por Suspicious Activity Report) a ser implementado por todas las entidades bancarias de los Estados Unidos. Los bancos tienen la obligación de radicar un ROS cada vez que detecten o sospechen violaciones de las leyes federales o transacciones sospechosas relacionadas con el lavado de dinero o con violaciones a la Ley del Secreto Bancario.

[3] Bajo la Ley del Secreto Bancario [o BSA, por su sigla en inglés], según la implementación de la misma que

hace [la sección] 31 CFR 103.11, el término "banco" incluye a todo agente, agencia, sucursal u oficina en Estados Unidos de bancos comerciales, corporaciones de ahorro y vivienda, entidades de ahorro y crédito, cooperativas de crédito y bancos extranjeros.

[4] 12 USC 1818(s) y 1829b, respectivamente.

Como respuesta a los ataques terroristas del 11 de septiembre de 2001, el Congreso de Estados Unidos promulgó la Ley de 2001 sobre la Unificación y Fortalecimiento de los Estados Unidos mediante el Suministro de Herramientas Apropiadas para Interceptar y Obstruir el Terrorismo (Ley Patriota). El Título III de la Ley Patriota es la Ley de Reducción del Lavado de Dinero Internacional y Lucha contra la Financiación del Terrorismo de 2001 [International Money Laudering Abatement and Anti-Terrorist Financing Act]. La Ley Patriota es sin duda la más importante legislación contra el lavado de dinero aprobada por el Congreso de los Estados Unidos desde la misma Ley del Secreto Bancario. Entre otras cosas, la Ley Patriota penalizó la financiación del terrorismo y amplió el marco de la Ley del Secreto Bancario al fortalecer los procedimientos de identificación de clientes; prohibirle a las entidades financieras negociar con bancos ficticios [bancos fachada] extranjeros; exigirle a las entidades financieras llevar a cabo procedimientos de debida diligencia, y en algunos casos, procedimientos de debida diligencia mejorados [o más detallados], a las cuentas de bancos corresponsales extranjeros y cuentas de banca privada de extranjeros; y mejorar el intercambio de información entre las entidades financieras y el Gobierno de los Estados Unidos. Así mismo, la Ley Patriota y su reglamentación también:

. • extendieron los requisitos fijados por el programa AML a todas las entidades financieras[5] (ver el Apéndice D (“Definición estatutaria de entidad financiera”) para mayor claridad);
. • aumentaron las sanciones civiles y penales fijadas al lavado de dinero;
. • autorizaron al Secretario del Tesoro de los Estados Unidos a imponer "medidas especiales" a jurisdicciones, instituciones o transacciones que revistan “interés fundamental en cuanto al lavado de dinero";
. • facilitaron el acceso a los registros documentales y obligaron a los bancos a responder las solicitudes regulatorias de información en un plazo de 120 horas;

• obligaron a las agencias bancarias federales a tomar en cuenta la trayectoria AML de los bancos en la revisión de posibles [casos de] fusiones y adquisiciones bancarias y otras aplicaciones relativas a combinaciones empresariales.

EL PAPEL DE LAS ENTIDADES OFICIALES CON RESPECTO A LA LEY DEL SECRETO BANCARIO (BSA)

Algunas entidades oficiales [de EE. UU.] juegan un papel clave en la implementación de las reglas de la Ley del Secreto Bancario, la elaboración de guías y pautas para los exámenes y el cumplimiento y el control de la Ley del Secreto Bancario. Estas entidades incluyen al Departamento del Tesoro de los Estados Unidos, FinCEN y las agencias bancarias federales (Junta de Gobernadores del Sistema de la Reserva Federal, Corporación Federal de Seguros de Depósitos [Federal Deposit Insurance Corporation], Administración

Nacional de Cooperativas de Crédito [National Credit Union Administration], Oficina del Contralor de la Moneda [Office of the Comptroller of the

[5] La Ley Patriota amplió el requerimiento del programa AML [de Lucha contra el lavado de dinero] a todas las entidades financieras, según se define dicho término en 31 USC 5312(a)(2). Sin embargo, para la fecha de la publicación del presente manual, tan sólo ciertos tipos de entidades financieras estaban sujetas a la reglamentación definitiva que implementa los requerimientos del programa AML formulados en 31 USC 5318(h)(1), según lo establecido por la Ley Patriota. Las entidades financieras que no están sujetas actualmente a una regla definitiva del programa AML están temporalmente exentas de los requisitos fijados en la Ley Patriota en cuanto a la creación de un programa AML, según se establece en 31 CFR 103.170.

Currency] y la Oficina de Supervisión de Entidades de Ahorro y Crédito [Office of Thrift Supervision]). A nivel internacional existen varias entidades oficiales multilaterales que apoyan la lucha contra el lavado de dinero y la financiación del terrorismo; ver el Apéndice E ("Organizaciones internacionales") para obtener información adicional.

Departamento del Tesoro de los Estados Unidos

La Ley del Secreto Bancario autoriza al Secretario del Tesoro a exigirle a las entidades financieras que establezcan programas AML [de lucha contra el lavado de dinero], radicar ciertos informes y mantener ciertos registros de transacciones. Algunas disposiciones de la Ley del Secreto Bancario se han ampliado para cubrir no sólo a las instituciones de depósito tradicionales, tales como bancos, asociaciones de ahorro y crédito y cooperativas de crédito, sino también entidades financieras no bancarias tales como negocios de servicios de dinero, casinos, agentes y comisionistas de títulos valores y comisionistas del mercado de futuros [futures commission merchants].

FinCEN

FinCEN, oficina adscrita al Departamento del Tesoro de Estados Unidos, es la entidad delegada para administrar la Ley del Secreto Bancario. FinCEN expide regulaciones así como guías interpretativas, lleva a cabo actividades de difusión con la industria regulada, apoya funciones relacionadas con los exámenes que llevan a cabo las agencias bancarias federales, e instaura acciones civiles cuando ello se requiere. En cada jurisdicción respectiva, FinCEN depende de las agencias bancarias federales para el examen de la banca sobre el cumplimiento con la Ley del Secreto Bancario. Otras obligaciones importantes de FinCEN incluyen ofrecer servicios de investigaciones de apoyo en casos judiciales, identificar e informar sobre tendencias y patrones que presentan los delitos financieros y promover la cooperación internacional con todas sus contrapartes a nivel mundial.

Agencias bancarias federales

Las agencias bancarias federales tienen la responsabilidad de vigilar las diferentes entidades bancarias que operan en Estados Unidos, incluyendo las sucursales en el extranjero de bancos de Estados Unidos. Las agencias bancarias federales tienen a su cargo la aprobación y acreditación (a través de NCUA, OCC y OTS), los seguros (a través de

FDIC y NCUA) y la regulación y supervisión de la banca [estadounidense][6]. Las sección 12 USC 1818 (s)(2) requiere que la agencia bancaria federal respectiva incluya una revisión del programa de cumplimiento de la Ley del Secreto Bancario en cada examen [o inspección] de una entidad de depósito [depositary institution] asegurada. Las agencias bancarias federales pueden hacer uso de su autoridad, según la

[6] La Junta de Gobernadores del Sistema de la Reserva Federal, la Corporación Federal de Seguros de Depósitos [Federal Deposit Insurance Corporation] y la Oficina de Supervisión de Entidades de Ahorro y Crédito [Office of Thrift Supervisión] pueden colaborar con las agencias bancarias estatales [es decir, de los Estados que hacen parte de los Estados Unidos] en cuanto al examen, la supervisión y el control BSA/AML en el caso de bancos constituidos bajo [las leyes de] los Estados de los Estados Unidos o acreditados por las autoridades de los mismos.

Las agencias bancarias federales requieren que cada banco bajo su supervisión establezca y mantenga un programa de cumplimiento con la Ley del Secreto Bancario.[7] Según la Ley Patriota los reglamentos de FinCEN requieren que algunas entidades financieras establezcan un programa de cumplimiento con la lucha contra el lavado de dinero que proteja contra el mismo y contra la financiación del terrorismo y asegure el cumplimiento de la Ley del Secreto Bancario y su reglamentación. Cuando se aprobó la Ley Patriota, los bancos supervisados por las agencias bancarias federales ya tenían la obligación legal de establecer y mantener un programa de cumplimiento con dicha ley, la cual, entre otras cosas, le exigía a los bancos identificar y reportar prontamente toda operación sospechosa. Por esta razón, la sección 31 CFR 103.120 sostiene que los bancos sujetos a regulación por las agencias bancarias federales cumplen con los requisitos del programa AML fijados en la Ley Patriota cuando desarrollan y mantienen un programa de cumplimiento con la Ley del Secreto Bancario que cumple con los requisitos del ente regulador federal funcional[8] que rige dichos programas. En el presente manual los requisitos del programa de cumplimiento con la Ley del Secreto Bancario que son del caso para cada agencia bancaria federal se denominan "el programa de cumplimiento BSA/AML".

Los bancos deben adoptar medidas razonables y prudentes para combatir el lavado de dinero y la financiación del terrorismo y minimizar así su vulnerabilidad a los riesgos inherentes a dichas actividades. Algunas organizaciones bancarias han visto cómo se afecta su reputación y han incurrido en sanciones monetarias civiles por no aplicar medidas de control apropiadas y haber incumplido con los requisitos de la Ley del Secreto Bancario. Además, puesto que el requisito de la lucha contra el lavado de dinero hace parte del trámite de la solicitud, todo lo que esté relacionado con BSA/AML puede afectar el plan estratégico del banco. Por esta razón, el compromiso de las agencias bancarias federales y de FinCEN con la entrega de pautas y guías que puedan ayudarle a los bancos a cumplir con la Ley del Secreto Bancario constituye una alta prioridad en términos de supervisión.

Las agencias bancarias federales quieren estar seguras de que las entidades que supervisan comprendan la importancia que tiene la existencia de un programa de cumplimiento BSA/AML. La gerencia debe estar alerta en este sentido, especialmente a medida que crece el negocio y se introducen nuevos productos y servicios. La evaluación del programa de cumplimiento de los bancos con BSA/AML y con los requisitos regulatorios de la Ley del

Secreto Bancario han sido parte integral del proceso de supervisión durante varios años. Ver el Apéndice A ("Legislación y reglamentación BSA") para conocer más información.

Ver 12 CFR 208.63 (Junta de Gobernadores del Sistema de la Reserva Federal); 12 CFR 326.8 (Corporación Federal de Seguros de Depósitos); 12 CFR 748.2 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Contralor de la Moneda); y 12 CFR 563.177 (Oficina de Supervisión de Entidades de de Ahorro y Crédito).

[8] Regulador Funcional Federal significa lo siguiente: Junta de Gobernadores del Sistema de la Reserva Federal; Corporación Federal de Seguros de Depósitos; Administración Nacional de Cooperativas de Crédito; Oficina del Contralor de la Moneda; Oficina de Supervisión de Entidades de Ahorro y Crédito; Comisión de Vigilancia y Control del Mercado de Valores [Securities and Exchange Commission]; o la Comisión de Comercio en Futuros de Bienes Básicos [Commodity Futures Trading Commission].

Como parte de un buen programa de cumplimiento BSA/AML, las agencias bancarias federales quieren asegurarse de que los bancos cuenten con políticas, procedimientos y procesos que les permitan identificar y reportar transacciones sospechosas a las autoridades. Los procesos de supervisión de dichas agencias determinan si los bancos han establecido políticas, procedimientos y procesos apropiados, según el propio riesgo BSA/AML de cada banco, para identificar y reportar operaciones sospechosas e incluir suficiente información detallada en los informes dirigidos a las autoridades para que éstos contribuyan a la investigación de las transacciones sospechosas reportadas. Ver los apéndices B ("Directivas BSA/ AML") y C (" Referencias BSA/ AML") para mayor información.

OFAC

La OFAC administra y vela por el cumplimiento de las sanciones económicas y comerciales derivadas de la política exterior de los Estados Unidos y sus objetivos de seguridad nacional; dichas sanciones económicas y comerciales están dirigidas a ciertos países, terroristas y narcotraficantes internacionales, así como a quienes participen en actividades relacionadas con la proliferación de armas de destrucción masiva. La OFAC actúa según las facultades especiales otorgadas al Presidente de Estados Unidos en tiempos de guerra o de emergencia nacional, así como bajo la autorización otorgada por actos legislativos específicos, que le permiten imponer controles a las transacciones y congelar los activos que estén bajo la jurisdicción de EE. UU. Muchas de las sanciones se basan en mandatos de la ONU y otros mandatos internacionales, son multilaterales en cuanto a su alcance, e incluyen estrecha cooperación con gobiernos aliados.

Los requisitos que establece la OFAC son distintos a los de la Ley del Secreto Bancario [BSA], pero tanto la OFAC como dicha Ley comparten un objetivo común de seguridad nacional. Por esta razón, muchas entidades financieras consideran que el cumplimiento con las sanciones de la OFAC está relacionado con el cumplimiento de las obligaciones fijadas por la Ley del Secreto Bancario; y el examen y la supervisión del cumplimiento con la Ley del Secreto Bancario tienen una conexión lógica con el examen del cumplimiento de las entidades financieras con las sanciones de la OFAC. Ver la sección de visión general fundamental titulada "Oficina de Control de Activos Extranjeros" en la página 84 para una mayor orientación, y los procedimientos para el examen de cumplimiento con la OFAC en

LAVADO DE DINERO Y FINANCIACIÓN DEL TERRORISMO

La Ley del Secreto Bancario [BSA] se propone salvaguardar al sistema financiero de los Estados Unidos y a las entidades financieras que lo constituyen de los abusos que representan los delitos financieros, incluyendo el lavado de dinero, la financiación del terrorismo y otras operaciones financieras ilícitas. El lavado de dinero y la financiación del terrorismo son delitos financieros cuyas consecuencias sociales y financieras son potencialmente devastadoras. Desde las ganancias de los narcotraficantes hasta los activos que funcionarios extranjeros deshonestos saquean de las arcas oficiales, el producto de estas actividades delictivas puede corromper y en últimas desestabilizar comunidades y economías enteras. Las redes terroristas pueden facilitarse sus actividades si cuentan con los medios económicos para hacerlo así como con acceso al sistema financiero. Tanto en el lavado de dinero como en la financiación del terrorismo, Las organizaciones bancarias tienen la obligación de desarrollar, implementar y mantener programas efectivos contra el lavado de dinero, capaces de afrontar las estrategias siempre cambiantes de los lavadores de dinero y los terroristas, así como las que se propongan acceder al sistema financiero de los Estados Unidos. Un sólido programa de cumplimiento BSA/AML es fundamental para disuadir y prevenir este tipo de actividades en bancos y otras entidades financieras. Ver el Apéndice F ("Alertas sobre el lavado de dinero y la financiación del terrorismo") para conocer ejemplos de operaciones sospechosas que pueden indicar la presencia de lavado de dinero o financiación del terrorismo.

Lavado de dinero

El lavado de dinero es la práctica delictiva del procesamiento de fondos ilícitos o dinero "sucio" mediante una serie de transacciones que permiten "limpiar" dichos fondos para que parezcan ser el resultado de actividades lícitas. El lavado de dinero generalmente no implica participación de dinero en todas las etapas del proceso. Aunque se trata de un proceso diverso y con frecuencia complejo, básicamente incluye tres pasos separados que también pueden darse en forma simultánea:

Colocación: La primera y más vulnerable etapa del proceso de lavado de dinero es la colocación del mismo. El objetivo es introducir fondos ilícitos en el sistema financiero sin atraer la atención de las entidades financieras ni las autoridades. Las técnicas empleadas incluyen organizar depósitos de moneda en montos que permitan evadir los requisitos de informes o mezclar depósitos de dineros ilícitos con dineros provenientes de actividades lícitas. Como ejemplos se pueden mencionar: dividir grandes sumas de dinero en pequeñas sumas menos conspicuas, que se depositan directamente en cuentas bancarias; depositar cheques de reembolso de paquetes vacacionales o pólizas de seguros canceladas; o adquirir una serie de instrumentos monetarios (por ejemplo, cheques de gerencia u giros postales) que luego se recaudan y depositan en las cuentas de otra sede u otra entidad financiera (ver el Apéndice G sobre "Estructuración" para conocer guías o pautas adicionales).

Distribución: La segunda etapa del proceso de lavado de dinero consiste en trasladar los

fondos dentro el sistema financiero. Se suele hacer mediante una serie de transacciones complejas que buscan generar confusión y complicar el respectivo rastro documental. Algunos ejemplos de esta distribución incluyen cambiar instrumentos monetarios por montos mayores o menores o girar o transferir fondos desde y hacia numerosas cuentas en una o más entidades financieras.

Integración: La finalidad última del proceso de lavado de dinero es la integración. Una vez los fondos han ingresado al sistema financiero y ha sido posible aislarlos en la etapa de la distribución, se emplea la etapa de integración para generar la apariencia de legalidad mediante una serie de transacciones adicionales. Estas transacciones brindan mayor protección a los delincuentes contra posibles nexos documentales y de registros con los fondos en cuestión, al ofrecer una explicación plausible del origen de los

Financiación del terrorismo

La motivación que conduce a la financiación del terrorismo es de tipo ideológico y contrasta con la búsqueda de ganancias que generalmente constituye el móvil de la mayoría de los delitos asociados al lavado de activos. Mediante la amenaza de la violencia, el terrorismo busca intimidar a una población u obligar a un gobierno u organización internacional a realizar ciertos actos o impedir la realización de ciertos actos. Las operaciones terroristas requieren una estructura financiera eficaz. Los grupos terroristas desarrollan fuentes de financiación relativamente móviles para asegurar los fondos que necesitan para obtener los insumos materiales y otros elementos logísticos empleados en los actos terroristas. Por lo tanto el lavado de dinero con frecuencia constituye un componente vital de la financiación del terrorismo.

Los terroristas generalmente financian sus actividades a través de fuentes legítimas así como ilegítimas. Las actividades ilegítimas, tales como la extorsión, el secuestro y el narcotráfico, han constituido una importante fuente de financiación. Otras actividades observadas incluyen el contrabando, fraude, hurto, robo, robo de identidad, empleo de "diamantes de conflicto"[9] y uso indebido de fondos de beneficencia o de asistencia humanitaria. En este último caso, es posible que los donantes ignoren que sus donaciones han sido desviadas para apoyar causas terroristas.

Otras fuentes legítimas también han sido utilizadas como fuente de financiación de organizaciones terroristas; estas constituyen una diferencia clave entre quienes financian el terrorismo y las organizaciones criminales tradicionales. Además de las donaciones de beneficencia, otras fuentes legítimas incluyen gobiernos extranjeros patrocinadores, la propiedad de empresas y el empleo personal.

Aunque los móviles que tienen los lavadores de dinero tradicionales y quienes financian el terrorismo varían, los métodos empleados en la práctica para financiar operaciones terroristas pueden ser los mismos o similares a los que emplean otros delincuentes que lavan fondos. Por ejemplo, quienes financian el terrorismo usan el contrabando de moneda, depósitos estructurados o retiros de cuentas bancarias, adquisiciones de varios tipos de instrumentos monetarios, tarjetas de crédito o débito o de valor almacenado, y

transferencias de fondos. También hay evidencia que indica que algunos tipos de banca informal (por ejemplo, los [procedimientos de remesas conocidos como] "hawala"[10])

[9] Los "diamantes de conflicto" se originan en áreas que están controladas por fuerzas o facciones opuestas a los gobiernos legítimos e internacionalmente reconocidos, y se emplean para financiar acciones militares contra dichos gobiernos o acciones que son contrarias a las decisiones del Consejo de Seguridad de las Naciones Unidas (www.un.org).

[10] "Hawala" se refiere a un tipo específico de sistema informal de transferencia de valor. FinCEN describe el sistema hawala como "un método de transmisión de valor monetario empleado en algunas partes del mundo para efectuar remesas, principalmente en el caso de quienes se proponen enviar dinero legítimamente a sus familiares en sus países de origen. También se ha observado que el sistema hawala y otros sistemas similares pueden están siendo utilizados como conductos para la financiación del terrorismo y otras actividades ilegales". Para conocer información adicional y guías sobre los sistemas de hawalas, así como el reporte elaborado por FinCEN para el Congreso [de los Estados Unidos] de conformidad con la sección 359 de la Ley Patriota, ver el sitio web de FinCEN en www.fincen.gov.

también han jugado un papel en la transferencia de fondos empleados por terroristas. Las transacciones realizadas a través de hawalas son difíciles de detectar debido a la ausencia de documentación, el tamaño de las mismas y la naturaleza de las respectivas transacciones. La financiación de ataques terroristas no siempre requiere grandes sumas de dinero, y las transacciones respectivas no necesariamente son complejas.

Sanciones penales al lavado de dinero, la financiación del terrorismo y las violaciones a la Ley del Secreto Bancario

Las sanciones que acarrea el lavado de dinero y la financiación del terrorismo pueden ser severas. Una persona hallada culpable de lavado de dinero puede enfrentar hasta 20 años de prisión y multas de hasta US $ 500.000[11]. Todas las propiedades involucradas en transacciones relacionadas con el producto de actividades criminales, o que se puedan rastrear a dicho producto, incluyendo propiedades tales como garantías prendarías, propiedades personales y en ciertos casos cuentas bancarias enteras (incluso si parte del dinero de esas cuentas es legítimo), pueden estar sujetas a confiscación[12]. De conformidad con una variedad de leyes, tanto bancos como personas naturales pueden incurrir en responsabilidad penal y civil por violación de la legislación contra el lavado de dinero y la financiación del terrorismo. Por ejemplo, según la Sección 18 USC 1956 y 1957, el Departamento de Justicia [de EE. UU.] puede instaurar acciones penales por lavado de dinero que pueden incluir sanciones penales, encarcelamiento y acciones dirigidas a la confiscación. Además, los bancos pueden perder su acreditación profesional y los empleados bancarios pueden perder sus empleos y quedar inhabilitados para trabajar en la banca.

Además, existen sanciones penales por violación intencional de la Ley del Secreto Bancario y su reglamentación bajo la sección 31 USC 5322 y por estructurar transacciones dirigidas a evadir los requisitos de informes que establece dicha Ley bajo 31 USC 5324(d). Por ejemplo, toda persona que viole intencionalmente la Ley del Secreto Bancario o su reglamentación, incluyendo empleados bancarios, está sujeta a sanciones penales de hasta

US $ 250.000 o cinco (5) años de prisión o ambas cosas[13]. La persona que cometa dicha violación mientras que simultáneamente viola otras leyes de los Estados Unidos o incurre en actividades delictivas, está sujeta a multas de hasta US $ 500.000 o diez (10) años de prisión o ambas cosas[14]. Los bancos que violen algunas de las disposiciones de la Ley del Secreto Bancario, incluyendo 31 USC 5318(i)
o (j), o medidas especiales impuestas bajo 31 USC 5318A, enfrentan sanciones penales monetarias de hasta US $ 1 millón o el doble del valor de la transacción respectiva, según lo que sea mayor[15].

Sanciones civiles a las violaciones de la Ley del Secreto Bancario

[11] 18 USC 1956.

[12] 18 USC 981 y 982.

[13] 31 USC 5322(a).

[14] Id [*Nota del traductor*: Ibid.]

[15] Id [*Nota del traductor*: Ibid.]
De conformidad con 12 USC 1818(i) y 31 USC 5331, las agencias bancarias federales y FinCEN, respectivamente, pueden instaurar acciones de sanción monetaria penal por violaciones a la Ley del Secreto Bancario. Además de las acciones de sanción monetaria penal y civil instauradas en su contra, es posible que a dichas personas se les retire de la banca de conformidad con 12 USC 1818(e)(2) por violaciones a dicha Ley bajo el Título 31 del Código de Estados Unidos, siempre que las violaciones no sean accidentales o no intencionales. Todas estas acciones están disponibles públicamente.
Visión general fundamental – Diseño del alcance y planeación

OBJETIVO

Identificar los riesgos que presenta el banco con respecto a la Ley del Secreto Bancario y la lucha contra el lavado de dinero y desarrollar el alcance y el plan del examen [o inspección]. Este examen incluye una determinación sobre las necesidades de personal para el examen, incluyendo experiencia y habilidades técnicas del mismo, y la selección de los procedimientos de examen a ser implementados.

VISIÓN GENERAL

El examen BSA/AML [sobre la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero] busca examinar la efectividad del programa de cumplimiento BSA/AML de los bancos así como el cumplimiento de los mismos con los requisitos regulatorios derivados

de la BSA, incluyendo una revisión de sus prácticas de gestión de riesgo.

PROCESO DE DISEÑO DEL ALCANCE Y LA PLANEACIÓN

Siempre que sea posible, se debe completar el proceso de diseño del alcance y la planeación antes de ingresar al banco. Durante este proceso puede ser útil comentar la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero con la gerencia del banco, incluyendo el oficial de cumplimiento respectivo, personalmente o por teléfono. El proceso de diseño del alcance y la planeación generalmente se inicia con un análisis de lo siguiente:

- Información de monitoreo desde fuera de la sede bancaria
- Informes y documentos de trabajo de exámenes previos
- Puntos de la carta de solicitud ya completados por la gerencia del banco. Ver el Apéndice H ("Puntos de la carta de solicitud") para obtener mayor información.
- La evaluación de riesgo BSA/AML del banco.
- Las bases de datos que almacenan la información de los informes sobre la Ley del Secreto Bancario (por ejemplo, el Currency and Banking Retrieval System (CBRS) [Sistema de recuperación de información de moneda y banca] y el Currency and Banking Query System (CBQS) [Sistema de consultas de moneda y banca]).
- Revisiones o auditorías independientes.

REVISIÓN DEL RIESGO BSA/AML DEL BANCO

Para lograr los objetivos del examen BSA/AML el examinador debe determinar el perfil de riesgo BSA/AML del banco, como parte del proceso de diseño del alcance y la planeación. Todo banco debe contar con un programa de cumplimiento BSA/AML diseñado para sus propios riesgos particulares. Al evaluar el nivel de riesgo, los bancos no deben basarse únicamente en un solo indicador para determinar la existencia de un riesgo mayor o menor. Deben también consultar a todas las líneas de negocios al preparar su evaluación de riesgo. El proceso de evaluación de riesgo debe tomar en cuenta una serie de factores, incluyendo la identificación del riesgo y la medición de los productos, servicios, clientes y ubicaciones geográficas. Además, la aplicación de estos factores depende de los hechos concretos respectivos, y la conclusión a que se llegue sobre el riesgo que presenta una cuenta debe estar fundamentada en la totalidad de la información disponible. Una evaluación de riesgo efectiva es un compuesto de múltiples factores, y dependiendo de las circunstancias, es posible que algunos factores pese en más que otros.

Esta evaluación de riesgo debe permitirle a los bancos administrar eficazmente el riesgo BSA/AML y por lo tanto es clave para el desarrollo de controles internos aplicables, como los requiere el programa de cumplimiento BSA/AML. Una descripción gráfica del vínculo que tiene el programa de cumplimiento BSA/AML con el proceso de evaluación de riesgo se suministra en el Apéndice I (“Relación de la evaluación de riesgo con el programa de cumplimiento BSA/AML”).

El proceso de diseño del alcance y la planeación debe guiarse por la revisión de la evaluación de riesgo BSA/AML del banco efectuada por el examinador. El examinador

debe revisar la evaluación de riesgo para determinar si está acorde con el riesgo que asume el banco. Si el banco no ha desarrollado una evaluación de riesgo, este hecho se debe tratar con la gerencia. Para los fines del examen, si el banco no ha completado su evaluación de riesgo o dicha evaluación es inadecuada, el examinador deberá completarla. La evaluación del riesgo debe incluir una revisión de todos los factores que son relevantes a la hora de determinar el perfil de riesgo particular que presenta un banco. El Apéndice J ("Matriz de cantidad de riesgo") incluye una guía para la evaluación del riesgo BSA/AML.

Evaluación del riesgo de las operaciones bancarias

Si bien los esfuerzos dirigidos a lavar dinero, financiar el terrorismo o realizar otras actividades ilegales a través de la banca pueden provenir de múltiples fuentes diferentes, algunos productos, servicios, clientes y ubicaciones geográficas pueden ser más vulnerables e históricamente presentan mayor abuso por parte de lavadores de dinero y delincuentes. Dependiendo de las características específicas del producto, servicio o cliente en particular, los riesgos no siempre serán los mismos. Varios factores, tales como el número y volumen de dólares, la ubicación geográfica y la presencia de clientes
o de quienes no lo son se deben tomar en cuenta en la evaluación de riesgo. Debido a las diferencias que se presentan entre estas variables, los riesgos pueden variar de banco en banco. Al formular un programa de cumplimiento BSA/AML, la gerencia debe identificar los riesgos importantes que corre el banco y desarrollar una evaluación de riesgo adaptada a las circunstancias particulares del banco.

Los programas de cumplimiento BSA/AML controlan los riesgos inherentes a los productos, servicios, clientes y ubicaciones geográficas únicas que tiene un banco. A medida que se introducen nuevos productos y servicios y cambian los actuales, y el banco se extiende a través de fusiones y adquisiciones, la evaluación gerencial del lavado de dinero y la financiación del terrorismo también debe evolucionar. Además, aún sin dichos cambios, todo banco debe revaluar periódicamente sus riesgos BSA/AML. Las secciones ampliadas del presente documento presentan una guía así como discusiones sobre líneas de negocios y productos específicos que pueden presentar retos únicos así como grados o niveles de exposición para los cuales los bancos deben instituir políticas, procedimientos y procesos adecuados. Si no se Productos y Servicios

Algunos productos y servicios que ofrecen los bancos representan un mayor riesgo de lavado de dinero o financiación del terrorismo, dependiendo de la naturaleza del producto o servicio específico de cada banco. Estos productos y servicios pueden facilitar un mayor grado de anonimidad, o manejar volúmenes más elevados de moneda
o su equivalente. A continuación se presenta una lista parcial de estos productos y servicios:

. • Servicios electrónicos de pagos de fondos --efectivo electrónico (tarjetas de valor almacenado y tarjetas de nómina), transferencias de fondos (nacionales e internacionales), transacciones pagaderas mediante presentación de identificación apropiada (PUPID, para Payable Upon Proper Identification), procesadores de pagos de terceros, remesas, compensación automatizada (ACH, para Automated Clearing House) y cajeros automáticos (ATM).

. • Banca electrónica
. • Banca privada, tanto nacional como internacional
. • Servicios fiduciarios y de administración de activos
. • Instrumentos monetarios[16]
. • Cuentas de corresponsalía extranjeras—transporte de valores bancarios [pouch activities], cuentas empleadas para pagos [payable through accounts] y letras de cambio en dólares de Estados Unidos.
. • Financiación del comercio internacional (cartas de crédito)
. • Préstamos, especialmente préstamos garantizados con efectivo, títulos o valores comerciales y préstamos sobre tarjetas de crédito.
. • Servicios de cuentas de no depósito (por ejemplo, productos de inversión que no son para depositar, seguros y casillas de seguridad).

Clientes y Entidades

Si bien todo tipo de cuenta es vulnerable al lavado de dinero y la financiación del terrorismo, algunos clientes y entidades constituyen riesgos concretos de lavado de dinero debido a la naturaleza de sus negocios, su ocupación o las transacciones que les son previsibles. Sin embargo, es indispensable que los bancos hagan uso de su buen criterio para no definir ni tratar a todos los miembros de una categoría concreta de clientes como si todos presentaran el mismo nivel de riesgo. Al evaluar el riesgo de los clientes, es fundamental que los bancos también consideren otras variables tales como los servicios que se solicitan, la fuente de los fondos y la ubicación geográfica. En cualquier categoría de negocios siempre habrá cuenta habientes que presenten algunos niveles de riesgo de lavado de dinero. Las secciones ampliadas del presente documento ofrecen una guía detallada así como discusiones sobre los siguientes clientes y entidades concretas:

Los instrumentos monetarios en este contexto incluyen cheques oficiales de bancos, cheques de gerencia, giros postales y cheques viajeros. Ver la sección de visión general ampliada titulada "Compraventa de instrumentos monetarios" en la página 123 para conocer información adicional sobre los factores de riesgo y la mitigación de riesgo en el caso de los instrumentos monetarios.

. • Entidades financieras extranjeras, incluyendo bancos y proveedores de servicios en moneda extranjera (por ejemplo, casas de cambio y *exchange houses,* reemisores de dinero y *bureaux de change*).
. • Entidades financieras no bancarias (por ejemplo, empresas de servicios de dinero, casinos y clubes de tarjetas, intermediarios y comisionistas de títulos valores y comerciantes en metales y piedras preciosas y joyas).
. • Políticos extranjeros de alto nivel y los miembros de sus familias inmediatas y su círculo de colaboradores inmediatos (colectivamente conocidos como personalidades sujetas a exposición política (PEP en inglés))[17].
. • Extranjeros no residentes[18] (NRA en inglés) y cuentas de ciudadanos extranjeros
. • Corporaciones extranjeras con cuentas de transacción, particularmente corporaciones extraterritoriales (tales como sociedades de inversión privada (Private Investment Companies – PIC) y corporaciones de negocios internacionales[19] (international business corporations – IBC) ubicadas en localidades geográficas de alto riesgo.

. • Intermediarios de depósito, particularmente intermediarios de depósito extranjeros
. • Negocios intensivos en efectivo (por ejemplo, “rapitiendas” [conveniente stores], restaurantes, almacenes minoristas, almacenes de venta de licores, distribuidores de cigarrillos, cajeros automáticos de propiedad privada, operadores de máquinas que venden refrigerios, y garajes de estacionamiento de vehículos).
. • Organizaciones no gubernamentales y entidades de beneficencia (extranjeras y nacionales)
. • Prestadores de servicios profesionales (por ejemplo, abogados, contadores, médicos

o agentes de finca raíz).

Ubicaciones Geográficas

Identificar las ubicaciones geográficas que representan mayor riesgo es fundamental para los programas de cumplimiento BSA/AML de los bancos. Los bancos estadounidenses deben entender y evaluar el riesgo concreto que implica realizar negocios en ciertas ubicaciones geográficas, abrirle cuentas a clientes provienentes de dichas ubicaciones y facilitar transacciones relacionadas con las mismas. Sin embargo, el riesgo geográfico en sí mismo no siempre determina el nivel de riesgo que puede presentar una entidad o una transacción, sea éste positivo o negativo.

Las ubicaciones geográficas de alto riesgo se pueden categorizar como internacionales o nacionales. Las internacionales generalmente incluyen lo siguiente:

[17] Favor referirse a la visión general ampliada titulada “Personas políticamente expuestas” ubicada en la página 153 para conocer pautas adicionales.

[18] Es posible identificar las cuentas de los Extranjeros No Residentes (NRA por su sigla en inglés) si se obtiene una lista de los clientes de las entidades financieras que han radicado formularios W-8. Para mayor información consultar el sitio www.irs.gov/formspubs.

[19] Para conocer una explicación de los PIC y los IBC, así como pautas adicionales al respecto, leer la visión general ampliada titulada “Entidades corporativas (nacionales y extranjeras)” en la página 164.

. • Países sujetos a las sanciones de la OFAC, incluyendo a Estados que patrocinan el terrorismo[20];
. • Países que han sido identificados como fuente de apoyo al terrorismo internacional bajo la sección 6(j) de la Ley de Administración de Exportaciones de EE. UU. [US Export Administration Act] de 1979, según lo que determine el Secretario de Estado[21];
. • Las jurisdicciones clasificadas como "de interés principal con respecto al lavado de dinero" por parte del Secretario del Tesoro de Estados Unidos, y las jurisdicciones sujetas a medidas especiales impuestas por el Secretario del Tesoro de los Estados Unidos, a través de FinCEN, de conformidad con la sección 311 de la Ley

Patriota[22].

. • Las jurisdicciones y países identificados como no cooperantes por el Grupo de Acción Financiera sobre Lavado de Dinero (GAFI) (Financial Action Task Force – FAFT)[23].

. • Importantes países y jurisdicciones de lavado de dinero identificados por el Informe Anual de Estrategia para el Control Internacional de Narcóticos de EE. UU. (IAECIN) (Internacional Narcotics Control Strategy Report – INCSR); concretamente, los países que han sido identificados como jurisdicciones de interés primordial[24].

. • Centros financieros extraterritoriales (OFC – Offshore Financial Centers por su sigla en inglés) identificados por el Departamento de Estado de Estados Unidos[25].

20

En el sitio web de la OFAC se puede ver una lista de estos países, jurisdicciones y gobiernos: www.treas.gov/ofac.

[21] En el informe anual del Departamento de Estado titulado "Patrones de terrorismo global" aparece una lista de los países que apoyan el terrorismo internacional. Este informe está disponible en el sitio web de la Oficina de Lucha Contra el Terrorismo [Counterterrorism Office] del Departamento de Estado, en www.state.gov/s/ct/.

[22] Las notificaciones sobre reglamentaciones propuestas y reglamentación definitiva que acompañan la determinación de ser "de interés principal con respecto al lavado de dinero" y la imposición de medidas especiales de conformidad con la sección 311 de la Ley Patriota, están disponibles en el sitio web de FinCEN en www.faft-gafi.org.

23

Una lista actualizada de los países que han sido designados por el GAFI [FAFT] como países y territorios no cooperantes (NCCT por su sigla en inglés) está disponible en el sitio web del GAFI en www.faft-gafi.org.

[24] El INCSR [Informe Anual de la Estrategia para el Control Internacional de Narcóticos], así como las listas de países y jurisdicciones que representan alto riesgo de lavado de dinero, se pueden consultar en el sitio de Internet del Departamento de Estado de los Estados Unidos (www.state.gov), en la página de la Oficina de Narcóticos Internacionales y Control Policial [Bureau of International Narcotics and Law Enforcement Affairs].

[25] Los OFC (Centros Financieros Extra-territoriales, Offshore Financial Centers) ofrecen una variedad de productos y servicios. Típicamente se trata de jurisdicciones con un número relativamente alto de entidades financieras dedicadas principalmente a realizar negocios con no residentes. Los OFC generalmente ofrecen todos o algunos de los siguientes servicios: cero impuestos o impuestos muy bajos; regulación financiera limitada; y secreto y anonimato bancario. Algunos OFC ofrecen la posibilidad de conformar y mantener una variedad de entidades jurídicas tales como Corporaciones de Negocios Internacionales [IBC – International Business Corporations], empresas "exentas", fideicomisos, fondos de inversión y empresas de seguros. Para mantener el anonimato del verdadero beneficiario del fideicomiso de dichas entidades, muchas se constituyen con directores, funcionarios y accionistas de fachada o interpuestos. Es posible que estas entidades financieras tengan muy poca o ninguna presencia en un OFC dado, y la actividad puede consistir únicamente en registrar la transacción. Para conocer más información, incluyendo evaluaciones de los OFC, ver el sitio de Internet www.imf.org/external/ns/cs.aspx?id=55.

• Otros países identificados por el banco como de alto riesgo debido a experiencia previa, historial de transacciones u otros factores (por ejemplo, consideraciones jurídicas o presunta corrupción oficial).

Las ubicaciones geográficas nacionales de alto riesgo pueden incluir oficinas

bancarias que realizan sus negocios en ubicaciones designadas por el Gobierno de Estados Unidos como de alto riesgo, o cuyos clientes están ubicados en dichas ubicaciones geográficas. Las ubicaciones geográficas nacionales de alto riesgo incluyen las siguientes:

- Zonas de Alta Densidad de Narcotráfico (HIDTA – High Intensity Drug Trafficking Areas)[26]
- Zonas de Alta Densidad de Delitos Financieros (HIFCA – High Intensity Financial Crime Area)[27]

PRUEBAS INDEPENDIENTES

Como parte de su proceso de diseño de alcance y planeación, los examinadores obtendrán y evaluarán los documentos de soporte de las pruebas independientes (auditoría)[28] del programa de cumplimiento BSA/AML del banco. El alcance y la calidad de la auditoría permitirán a los examinadores conocer los riesgos particulares que enfrenta el banco, ver cómo se están administrando y controlando estos riesgos, y el cumplimiento del banco con la Ley del Secreto Bancario. El alcance y los documentos de trabajo de las pruebas independientes ayudarán a los examinadores a comprender el cubrimiento de la auditoría así como la calidad y cantidad de las pruebas de transacciones. Esta información ayudará al examinador a determinar el alcance del examen e identificar áreas que requieren mayor (o menor) atención así como las ocasiones en que se requieran procedimientos de examen ampliados.

PLAN DEL EXAMEN

Como mínimo, los examinadores deben realizar los procedimientos que aparecen en las siguientes secciones del presente manual, para asegurar que el banco disponga de un programa de cumplimiento BSA/AML adecuado a su propio perfil de riesgo:

- Diseño de Alcance y Planeación (ver páginas 170 a 173)
- Programa de Cumplimiento BSA/AML (ver páginas 174 a 178)
- Conclusiones y Finalización del Examen (ver páginas 210 a 213).

[26] Se puede ver una lista de estas zonas en www.whitehousedrugpolicy.gov.

[27] Se puede ver una lista de estas zonas en www.irs.gov/compliance/enforcement/article/0,,id=107488,00html#hifca.

[28] La referencia a la "auditoría" que hacen las agencias bancarias federales no implica necesariamente que las pruebas independientes deban ser realizadas por un auditor interno o externo especialmente designado para el efecto. Sin embargo, la persona que realice las pruebas independientes no puede ser parte del programa de cumplimiento con la Ley del Secreto Bancario [BSA] y la Lucha contra el lavado de dinero [AML] del banco. Los resultados se deben reportar directamente a la junta directiva o a un comité de auditoría compuesto principal o totalmente por directores externos.
La parte del núcleo o principal incluye también una visión general y los procedimientos para el examen de las políticas, procedimientos y procesos del banco, con miras a asegurar su cumplimiento con las sanciones de la OFAC. El examinador debe revisar la evaluación

de riesgo OFAC del banco y hacer una auditoría para determinar hasta dónde es necesario revisar el programa OFAC del banco durante el proceso mismo del examen. Favor referirse a los procedimientos de la "Oficina de Control de Activos Extranjeros" en las páginas 207 a 209.

El examinador debe desarrollar un plan inicial de examen adecuado al perfil general de riesgo BSA/AML que presenta el banco. Este plan podrá cambiar durante el transcurso del examen, como resultado de los hallazgos hechos en el terreno. El examinador debe redactar una carta de solicitud dirigida al banco. En el Apéndice H ("Puntos de la carta de solicitud") se sugieren los puntos que debe incluir la carta de solicitud. Sobre la base del perfil de riesgo, la calidad de la auditoría, los resultados de los exámenes previos y el trabajo inicial de examen, los examinadores deben completar los procedimientos de examen fundamentales y ampliados, según se requiera. En las organizaciones bancarias más grandes y complejas los examinadores podrán completar varios tipos de exámenes durante el transcurso del plan o ciclo de supervisión. Estas revisiones podrán enfocarse en una o más líneas de negocios (por ejemplo, banca privada, financiación comercial o relaciones con bancos corresponsales extranjeros). El examinador debe incluir una evaluación del programa de cumplimiento BSA/AML del banco dentro del plan o ciclo de supervisión.

Pruebas de transacciones

Los examinadores llevan a cabo pruebas de transacciones para evaluar el cumplimiento del banco con los requisitos regulatorios, determinar la eficacia de las políticas, procedimientos y procesos del mismo, y evaluar sus sistemas de monitoreo de operaciones sospechosas. Las pruebas de transacciones son importantes en el momento de determinar las conclusiones sobre la integridad general de los controles y procesos de gestión de riesgo que ha implementado el banco. Las pruebas se deben realizar durante cada examen y pueden llevarse a cabo como parte de la sección de función de pruebas independientes (auditoría) o completando los procedimientos de pruebas de transacciones que aparecen en otras partes dentro de las secciones fundamentales o ampliadas. Cuando se llevan a cabo, la extensión de estas pruebas y actividades de transacciones depende de varios factores, incluyendo el propio juicio del examinador sobre los riesgos, controles e idoneidad de las pruebas independientes realizadas. Una vez en el terreno, se puede ampliar el alcance de las pruebas de transacciones para que incluyan aspectos o temas identificados durante el proceso del examen.

INFORMACIÓN OBTENIDA DE LAS BASES DE DATOS DE LOS INFORMES BSA [sobre la Ley del Secreto Bancario]

La planeación de los exámenes debe también incluir un análisis de los ROS o Reportes de operaciones sospechosas, CTR o Informes de transacciones en moneda y las exenciones respecto a éste último informe que haya radicado el banco. Los ROS, CTR y las exenciones de los CRT se pueden obtener directamente en línea de las bases de datos de los informes BSA (por ejemplo, CBRS y CBQS). Cada agencia bancaria federal cuenta con personal autorizado para obtener estos datos de las bases de datos de los informes BSA. Cuando

requiera efectuar búsquedas en las bases de datos de los informes BSA, el(la) examinador(a) debe ponerse en contacto con la(s) persona(s) indicada(s) en su agencia con suficiente anticipación a la fecha de inicio del examen para poder obtener la información solicitada. Cuando en fecha reciente un banco ha adquirido a otro banco o se ha fusionado con él, el examinador también debe obtener los informes ROS, CTR y exención de CTR del banco que ha sido adquirido.

La información descargada de Internet se puede mostrar en una hoja electrónica, con todos los datos que aparecen en el documento original radicado por el banco, así como con el Número de Control de Documento (DNC -Document Control Number) del Servicio de Ingresos Nacionales de Estados Unidos (IRS) [el ente tributario de ese país, cuya sigla corresponde a Internal Revenue Service], y la fecha en que el documento ingresó a la base de datos de informes BSA. La información descargada de Internet puede ser importante para el examen, por cuanto ayuda a los examinadores a:

. • Identificar clientes de altos volúmenes de moneda
. • Colaborar con la selección de cuentas para las pruebas de transacciones
. • Identificar el número y las características de los informes ROS radicados
. • Identificar el número y la naturaleza de las exenciones.

Visión general fundamental – Programa de cumplimiento BSA/AML

OBJETIVO

Evaluar si el programa de cumplimiento BSA/AML es adecuado. Determinar si el banco ha desarrollado, administrado y mantenido un programa eficaz de cumplimiento con la Ley del Secreto Bancario y con toda la reglamentación de la misma.

VISIÓN GENERAL

La revisión de las políticas, procedimientos y procesos fijados por escrito por el banco constituye el primer paso en la determinación de si el programa de cumplimiento BSA/AML del banco es apropiado en términos generales. Es necesario completar los procedimientos de examen fundamentales aplicables, y de ser necesario, los procedimientos ampliados, para sustentar las conclusiones generales a que se llegue respecto a si el programa de cumplimiento BSA/AML del banco es apropiado. Los resultados del examen deben discutirse con la gerencia, los resultados más importantes deben incluirse en el informe del examen.

EL PROGRAMA DE CUMPLIMIENTO BSA/AML

El programa de cumplimiento BSA/AML debe existir por escrito y haber sido aprobado por la Junta Directiva y registrado así en las actas de la misma. El programa de cumplimiento

BSA/AML de un banco debe corresponder al respectivo perfil de riesgo BSA/AML del mismo. Ver el Apéndice I (“Relación de la evaluación de riesgo con el Programa de cumplimiento BSA/AML”). Además, el programa se debe haber implementado plenamente y su diseño debe cumplir de manera razonable con los requisitos fijados en la Ley del Secreto Bancario. No bastan las declaraciones sobre políticas; las prácticas del banco deben coincidir con las políticas, procedimientos y procesos fijados por escrito por la entidad. El programa de cumplimiento BSA/AML debe incluir los siguientes requisitos mínimos:

. • Un sistema de controles internos para asegurar el cumplimiento continuo
. • Pruebas independientes de cumplimiento BSA/AML
. • Una(s) persona(s) designada(s) por el banco como responsable(s) de la gestión de cumplimiento con la Ley del Secreto Bancario (oficial de cumplimiento BSA)
. • Capacitación del personal apropiado

Además, el programa de cumplimiento BSA/AML debe incluir un Programa de identificación del cliente (CIP – Customer Identification Program). Ver la sección de visión general fundamental titulada "Programa de identificación del cliente" en la página 30 para obtener mayor información.

Controles internos

La junta directiva del banco, a través de la alta gerencia del mismo, es quien tiene la responsabilidad última de mantener una estructura interna eficaz de controles BSA/AML en el banco, incluyendo el monitoreo y la elaboración de informes sobre operaciones sospechosas. La junta directiva y la gerencia deben crear una cultura de cumplimiento para asegurar que el personal se adhiera a las políticas, procedimientos y procesos establecidos por el banco con respecto a BSA/AML. Los controles internos consisten en las políticas, procedimientos y procesos del banco que están diseñados para limitar y controlar los riesgos y lograr cumplir con la Ley del Secreto Bancario. El nivel de sofisticación de dichos controles internos debe ser acorde con la dimensión, estructura, riesgos y complejidad del banco. Los bancos grandes y complejos probablemente han fijado medidas de control interno de cumplimiento BSA/AML por departamentos. Los controles internos por departamentos típicamente están dirigidos a los requisitos de riesgo y cumplimiento únicos que presentan líneas de negocios o departamentos específicos, y hacen parte de un programa de cumplimiento BSA/AML general.

Los controles internos se deben encargar de las siguientes funciones:

. • Identificar las operaciones bancarias (productos, servicios, clientes y ubicaciones geográficas) que son más vulnerables al abuso por parte de lavadores de dinero y delincuentes; suministrar actualizaciones periódicas del perfil de riesgo del banco; y sustentar un programa de cumplimiento BSA/AML diseñado específicamente para gestionar los riesgos propios del banco.
. • Informar a la junta directiva o a un comité de la misma, al igual que a la alta gerencia, respecto a iniciativas de cumplimiento, deficiencias de cumplimiento que hayan sido identificadas, y medidas correctivas adoptadas, así como notificar a los directores y a la alta gerencia sobre todo Reporte de operaciones sospechosas (ROS) que haya sido

radicado[29].

. • Identificar a la(s) persona(s) que tenga(n) a su cargo el cumplimiento BSA/AML.

. • Asegurar la continuidad del programa pese a los cambios que puedan darse en la composición o estructura de la gerencia o de los empleados.

. • Cumplir con todos los requisitos de mantenimiento de datos y elaboración de informes, cumplir con las recomendaciones relativas al cumplimiento BSA/AML y llevar a cabo actualizaciones oportunas en respuesta a cambios regulatorios.

. • Implementar políticas, procedimientos y procesos de Debida diligencia del cliente (CDD – Customer Due Diligence) basados en el riesgo.

. • Identificar transacciones reportables y diligenciar correctamente todos los informes requeridos, incluyendo ROS, Informes de transacciones en moneda (CTR – Currency Transaction Reports) y exenciones de éstos últimos (los bancos deben contemplar la posibilidad de centralizar las funciones de revisión y diligenciamiento de informes dentro de la organización bancaria).

. • Disponer doble control y separación de obligaciones (los empleados que están encargados de diligenciar los formularios de los informes (por ejemplo los ROS, CTR y las exenciones de CTR) no deben ser los mismos que tienen a su cargo radicar los informes u otorgar las exenciones).

. • Establecer suficientes sistemas de control y monitoreo para una detección y elaboración de operaciones sospechosas y elaboración oportuna de los respectivos ROS.

[29] Las cooperativas de crédito [credit unions] no están sujetas al requisito regulatorio de notificar a la junta directiva sobre los ROS que radiquen, si bien muchas de ellas adoptan esta medida [de todas formas] como una “mejor práctica” ["best practice”].

. • Disponer una adecuada supervisión de los empleados encargados de manejar transacciones de moneda, diligenciar formularios, otorgar exenciones, monitorear operaciones sospechosas o participar en cualquier otra actividad cubierta por la Ley del Secreto Bancario y la regulación de la misma.

. • Agregar el cumplimiento con la Ley del Secreto Bancario a las descripciones de los cargos y evaluaciones de desempeño del personal apropiado.

Lo anterior no pretende ser exhaustivo y se debe ajustar al perfil de riesgo de cada banco. En las secciones ampliadas del presente manual se incluyen guías o pautas adicionales dirigidas a tratar el riesgo que presentan áreas específicas.

Pruebas independientes

Las pruebas independientes (auditorías) deben ser realizadas por el departamento de auditoría interna, auditores externos, consultores u otras partes independientes calificadas. Si bien la frecuencia de las auditorías no está definida específicamente en ninguna ley, una buena práctica consiste en que el banco lleve a cabo pruebas independientes al menos una vez al año. Los bancos que no emplean auditores ni consultores externos o que cuentan con departamentos de auditoría interna pueden cumplir con este requisito empleando personal calificado que no haga parte de las funciones que están siendo probadas. Las personas que llevan a cabo las pruebas BSA/AML deben reportar directamente a la junta directiva o a un

comité especialmente designados de la misma, compuesto principal o enteramente por directores externos.

Las personas encargadas de la evaluación objetiva e independiente del programa de cumplimiento BSA/AML fijado por escrito por el banco deben realizar pruebas para verificar el cumplimiento específico con respecto a la Ley del Secreto Bancario, y evaluar los sistemas de información de gestión (MIS – Management Information Systems) que sean relevantes. La auditoría debe fundamentarse en el riesgo[30] y evaluar la calidad de la gestión de riesgo en todas las operaciones, departamentos y subsidiarias del banco. Los programas de auditoría basados en riesgo pueden variar según el tamaño y la complejidad del banco y el alcance de sus actividades, su perfil de riesgo, la calidad de sus funciones de control, su diversidad geográfica y el uso que haga de la tecnología. Un programa de auditoría efectivo basado en riesgo cubre todas las actividades del banco. La frecuencia y profundidad de cada actividad de auditoría variará según la evaluación de riesgo de cada actividad. La auditoría basada en riesgo le permite a la junta directiva y a los auditores utilizar la evaluación de riesgo del banco para enfocar el alcance de la auditoría en las áreas de mayor preocupación. Las pruebas deben brindarle a la junta directiva y la gerencia la posibilidad de identificar áreas de debilidad o áreas que requieren mejoras o controles más fuertes.

Las pruebas independientes deben incluir lo siguiente, como mínimo:

. • Una evaluación de la integridad general y eficacia del programa de cumplimiento BSA/AML del banco, incluyendo sus políticas, procedimientos y procesos.
. • Una revisión de la adecuación de la evaluación de riesgo del banco al perfil de riesgo de la misma entidad (productos, servicios, clientes y ubicaciones geográficas).
. • Pruebas de transacciones adecuadas que permitan verificar el cumplimiento del banco con los requisitos de registros de datos y elaboración de informes de la Ley del Secreto Bancario (por ejemplo, CIP, SAR, CTR, exenciones de CRT, solicitudes de compartir información).
. • Una evaluación de los esfuerzos llevados a cabo por la gerencia del banco dirigidos a resolver violaciones y deficiencias observadas en auditorías y exámenes regulatorios previos, incluyendo avances con respecto al cumplimiento con requerimientos supervisorios que aún estén pendientes, si los hay.
. • Una revisión de la capacitación del personal enfocada en la idoneidad, precisión y lo integral que sea la misma.
• Una revisión de la eficacia de los sistemas de monitoreo de operaciones sospechosas (sistemas manuales, automatizados o una combinación de los mismos) empleados para el cumplimiento BSA/AML. Los respectivos informes pueden incluir lo siguiente, sin limitarse únicamente a ello:
-Informes de monitoreo de operaciones sospechosas -informes de agregación de grandes volúmenes de moneda -registros de instrumentos monetarios -registros de transferencias de fondos -reportes de fondos insuficientes -informes de grandes fluctuaciones de saldos -informes de las relaciones asociadas a las cuentas
. • Una evaluación del proceso general de identificación y elaboración de informes de operaciones sospechosas, incluyendo una revisión de los informes ROS ya radicados

[30] Favor referirse al Apéndice J ("Matriz de cantidad de riesgo").

o elaborados, para determinar la precisión y oportunidad de los mismos, así como determinar si están completos, y la efectividad de la política respectiva del banco.

Los auditores deben documentar el alcance de la auditoría, los procedimientos realizados, las pruebas de transacciones realizadas y los resultados de la revisión. Toda la documentación de la auditoría y los materiales de trabajo relativos a la misma deben ponerse a la disposición del examinador para su revisión. Toda violación, excepción en cuanto a políticas o procedimientos u otras deficiencias observadas durante la auditoría deben quedar incluidas en el informe de auditoría y reportadas ante la junta directiva o un comité oportunamente designado para tal efecto por la misma. La junta directiva o el Comité designado por la misma así como el personal de auditoría deben rastrear las deficiencias de auditoría y documentar acciones correctivas respectivas.

El Oficial de cumplimiento con la Ley del Secreto Bancario

La junta directiva del banco deberá designar a un empleado calificado como Oficial de Cumplimiento con la Ley del Secreto Bancario[31] [Oficial de Cumplimiento BSA]. El Oficial de Cumplimiento BSA está encargado de coordinar y monitorear el

[31] El banco debe designar a una o más personas para coordinar y monitorear el cumplimiento diario. Este requerimiento se detalla en las regulaciones del programa de cumplimiento BSA de las agencias bancarias federales: 12 CFR 208.63 (Junta de Gobernadores del Sistema de la Reserva Federal); 12 CFR 326.8 (Corporación Federal de Seguros de Depósitos); 12 CFR 748.2 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Contralor de la Moneda); y 12 CFR 563.177 (Oficina de Supervisión de Entidades de Ahorro y Crédito).

cumplimiento diario con BSA/AML. Dicho funcionario también tiene a su cargo todo lo relacionado con la administración del programa de cumplimiento BSA/AML y la gestión de adhesión por parte del banco a toda la reglamentación de las mismas. Sin embargo la junta directiva es quien tiene la responsabilidad última del cumplimiento BSA/AML del banco.

Si bien el cargo de la persona que tiene a su cargo el cumplimiento general BSA/AML del banco no es importante, el nivel de autoridad y responsabilidad de dicha persona dentro del banco si son fundamentales. El oficial de cumplimiento con la Ley del Secreto Bancario podrá delegar funciones BSA/AML en otros empleados, pero es el responsable del cumplimiento general BSA/AML del banco. La junta directiva tiene la responsabilidad de asegurarse de que el funcionario de cumplimiento cuente con suficiente autoridad y recursos (monetarios, físicos y de personal) para administrar un programa de cumplimiento BSA/AML eficaz conforme al perfil de riesgo del banco.

El oficial de cumplimiento con la Ley del Secreto Bancario debe conocer plenamente dicha ley y toda la reglamentación relativa a la misma. Dicho oficial también debe comprender los productos, servicios, clientes y ubicaciones geográficas del banco, y los riesgos potenciales de lavado de dinero y financiación del terrorismo que están asociados a estas

actividades. No basta con nombrar un oficial de cumplimiento BSA para cumplir con el requisito regulatorio si dicha persona carece de la experiencia, autoridad o tiempo que se requieren para cumplir con su trabajo a satisfacción.

Las comunicaciones deben permitirle al oficial de cumplimiento BSA informar regularmente a la junta directiva y a la alta gerencia sobre el desarrollo del cumplimiento BSA. Se debe reportar a la junta directiva o a un comité designado por la misma toda la información relativa a la BSA, incluyendo los informes ROS radicados ante FinCEN, para que dichas personas puedan tomar decisiones informadas sobre el cumplimiento general BSA/AML. El oficial de cumplimiento tiene la responsabilidad de ejecutar las instrucciones impartidas por la junta directiva y asegurarse de que los empleados se adhieran a las políticas, procedimientos y procesos BSA/AML del banco.

Capacitación

Los bancos deben asegurarse de que haya personal apropiado capacitado en los aspectos aplicables de la Ley del Secreto Bancario. La capacitación debe incluir los requisitos regulatorios así como las políticas, procedimientos y procesos BSA/AML internos del banco. Como mínimo, el programa de capacitación debe suministrar capacitación a todo el personal del banco cuyas obligaciones requieran conocimiento de la Ley del Secreto Bancario. Dicha capacitación debe estar diseñada para satisfacer las responsabilidades concretas de dicha persona. Además, se debe impartir a todo personal nuevo una visión general de los requisitos fijados por BSA/AML. La capacitación debe incluir información relativa a las líneas operacionales aplicables, tales como servicios fiduciarios, internacionales y banca privada.

Se debe informar a la junta directiva y la alta gerencia del banco sobre todo cambio y nuevos desarrollos relativos a BSA, la reglamentación y directivas de implementación de la misma, y la reglamentación de las agencias bancarias federales. Si bien la junta directiva no requiere el mismo grado de capacitación que debe ofrecerse al personal de operaciones del banco, si requiere la importancia que tienen los requisitos regulatorios BSA/AML, las implicaciones del incumplimiento de los mismos y los riesgos que enfrenta el banco. Si no entienden en términos generales la Ley del Secreto Bancario, la junta directiva no podrá supervisar correctamente el cumplimiento BSA/AML, ni aprobar las políticas, procedimientos y procesos BSA/AML, ni proveer suficientes recursos para ello.

La capacitación debe ser continua e incorporar desarrollos actuales así como cambios introducidos en la Ley del Secreto Bancario y toda reglamentación relacionada. Los cambios efectuados en las políticas, procedimientos, procesos y sistemas de monitoreo internos también deben quedar cubiertos por la capacitación. El programa debe reforzar la importancia que le otorgan la junta directiva y la alta gerencia al cumplimiento del banco con la Ley del Secreto Bancario y asegurarse de que todos los empleados comprendan su papel en el mantenimiento de un programa eficaz de cumplimiento BSA/AML.

Los ejemplos de las actividades de lavado de dinero y monitoreo y elaboración de informes sobre operaciones sospechosas pueden y deben diseñarse a la medida de cada auditorio

particular. Por ejemplo, la capacitación dirigida a quienes laboran como cajeros debe enfocarse en ejemplos de transacciones de montos elevados de moneda u otras operaciones sospechosas; la capacitación dirigida al departamento de préstamos debe dar ejemplos de lavado de dinero a través de distintos tipos de préstamos.

Los bancos deben documentar sus programas de capacitación y llevar registros de los mismos que incluyan los materiales de prueba, las fechas de las sesiones de capacitación y la asistencia a las mismas, y estos materiales deben estar a la disposición del examinador para su revisión.

Visión general fundamental – Programa de identificación del cliente

OBJETIVO

Evaluar el cumplimiento del banco con los requisitos estatutarios y regulatorios del Programa de identificación del cliente (CIP en inglés).

VISIÓN GENERAL

Desde el 1 de octubre de 2003 todos los bancos [de los Estados Unidos] y sus subsidiarias deben contar con un CIP consignado por escrito[32]. La norma sobre el CIP implementa la sección 326 de la Ley Patriota y requiere que cada banco aplique un CIP formulado por escrito, adaptado a su tamaño y tipo de negocios y que incluya ciertos requerimientos mínimos. El CIP debe quedar incorporado al programa de cumplimiento BSA/AML del banco, sujeto a la aprobación de la junta directiva del mismo[33].

El objetivo del CIP consiste en permitirle al banco creer razonablemente que conoce la verdadera identidad de cada uno de sus clientes. El CIP debe incluir procedimientos de apertura de cuenta que especifiquen la información de identificación que se debe obtener de cada cliente. También debe incluir procedimientos razonables y prácticos basados en riesgo que se usan para verificar la identidad de cada cliente. Los bancos deben evaluar los riesgos que implican su propia base de clientes y oferta de productos. Dicha evaluación debe considerar lo siguiente al determinar los riesgos:

. • El tipo de cuentas que se ofrecen
. • Los métodos empleados por el banco para la apertura de cuentas
. • Las distintos tipos de información de identificación disponibles
. • El tamaño, la ubicación y la base de clientes del banco.

De conformidad con la regla relativa al CIP, una "cuenta" es una relación bancaria formal de prestación o participación en servicios, negocios u otras transacciones financieras, e incluye una cuenta de depósito, una cuenta de transacciones o activos, una cuenta de crédito u otra extensión de crédito. Una cuenta también incluye una relación establecida para proveer casillas u otros servicios de seguridad o para ofrecer servicios de gestión de

efectivo, custodia o fiducia.

Una cuenta no incluye lo siguiente:

[32] Ver CFR 208.63(b), 211.24(m), 211.24(j) (Junta de Gobernadores del Sistema de la Reserva Federal); 12 CFR 326.8(b) (Corporación Federal de Seguros de Depósitos); 12 CFR 748.2(b) (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.21 (Oficina del Contralor de la Moneda); 12 CFR 563.177(b) (Oficina de Supervisión de Entidades de Ahorro y Crédito); y 31 CFR 103.121 (FinCEN).

[33] Para la fecha de publicación de este manual, los bancos privados no sujetos a regulación federal, las empresas de fideicomiso y cooperativas de crédito no están sujetas al requerimiento del programa de cumplimiento BSA/AML; sin embargo la junta directiva del banco de todas formas debe aprobar el Programa de identificación del cliente (CIP por su sigla en inglés).

. • Productos o servicios para los cuales no se establece una relación bancaria formal con una persona, tales como pago de cheques, transferencia de fondos o venta de cheques o de giros postales [money orders].

. • Cuentas adquiridas por el banco. Esto puede incluir cuentas sencillas o múltiples resultado de la compra de activos, adquisiciones, fusiones o por asumir pasivos.

. • Cuentas abiertas para participar en planes de beneficio de empleados creados bajo la Ley de Seguridad de Pensiones de Empleados [Employee Retirement Income Security Act] de 1974.

La regla sobre los CIP aplica a los "clientes". Un cliente es una "persona" (persona física o natural, corporación, asociación, fiducia, bienes patrimoniales [estate] o cualquier otra entidad reconocida como persona jurídica) que abre una cuenta; una persona natural que abre una cuenta en nombre de otra que persona natural que carece de personería jurídica; y una persona natural que abre una cuenta en nombre de una entidad sin personería jurídica (por ejemplo, un club cívico). La definición de cliente excluye a quienes no reciben servicios bancarios, como por ejemplo alguien a quien le haya sido negada una solicitud de crédito.[34] La definición de "cliente" tampoco incluye a los clientes actuales, siempre que el banco considere razonablemente que conoce la verdadera identidad de los mismos.[35] Quedan excluidos de esta definición de cliente los bancos que están sujetos a regulación federal, bancos regulados por el regulador bancario estatal [de los Estados de EE. UU.], las entidades oficiales y las compañías que se transan públicamente (según se describe en 31 CFT 103.22(d)(2)(ii) al (iv)).

INFORMACIÓN REQUERIDA DE LOS CLIENTES

El CIP debe incluir procedimientos de apertura de cuentas que detallen la información que se debe obtener de cada cliente[36]. Como mínimo, el banco debe obtener la siguiente información básica para poder abrir una cuenta[37]:

. • Nombre

. • Para personas naturales, fecha de nacimiento

Cuando la cuenta es un préstamo, se considera que ha sido "abierta" cuando el banco celebra un contrato ejecutable por medio del cual se compromete a ofrecerle un crédito al cliente.

[35] El banco puede demostrar que conoce la verdadera identidad de un cliente actual si demuestra que con anterioridad a la expedición de la regla CIP definitiva ya disponía de procedimientos similares utilizados para verificar la identidad de personas que tenían cuenta con el banco para el 1 de octubre de 2003, si bien es posible que el banco no haya recopilado exactamente la misma información sobre estas personas que solicita la regla CIP definitiva. Los procedimientos alternos incluyen demostrar que el banco tiene una larga y activa relación con una persona particular, evidenciada por ejemplo en la historia de extractos de cuenta enviados a dicha persona, información enviada al fisco [Servicio de Ingresos Nacionales] (IRS por su sigla en inglés) sobre las cuentas de la persona sin disputas [without issue], préstamos otorgados y pagados u otros servicios prestados a dicha persona a través del tiempo. Es posible que los medios alternativos, sin embargo, no resulten suficientes para aquellos que, según el banco, representan un alto riesgo.

[36] Cuando una persona natural abre una cuenta para una entidad que no tiene personería jurídica o para otra persona natural que carece de personería jurídica, se debe obtener la información que permita identificar a la persona que abre la cuenta.

[37] Para los clientes de tarjetas de crédito, antes de otorgar el crédito el banco puede obtener información de terceros que permita identificar al cliente.

. • Dirección[38]

. • Número de identificación[39].

Según sus evaluaciones de riesgo, los bancos pueden solicitar información de identificación adicional a los anteriores elementos para ciertos clientes o líneas de producto.

VERIFICACIÓN DE LOS CLIENTES

El CIP debe incluir procedimientos fundamentados en riesgo para verificar la identidad de los clientes durante un período de tiempo razonable luego de haber sido abierta la cuenta. Los procedimientos de verificación deben emplear "la información obtenida de conformidad con [31 CFR 103.121] párrafo (b)(2)(i)", es decir, la información de identificación obtenida por el banco. El banco no está obligado a determinar la precisión de cada uno de los elementos de la información de identificación obtenida, pero sí debe verificar suficiente información como para generar la creencia razonable de que conoce la verdadera identidad del cliente. Los procedimientos del banco deben describir en qué momento hará uso de documentos, métodos no basados en documentos o una combinación de los dos.

Verificación mediante documentos

Los bancos que emplean métodos documentales para verificar la identidad de los clientes deben contar con procedimientos que especifiquen el mínimo de documentos requeridos. La regla sobre el CIP ofrece ejemplos de tipos de documentos que durante mucho tiempo han sido considerados como fuentes primarias de identificación, y refleja la expectativa que tienen las agencias bancarias federales en el sentido de que, con la mayoría de sus clientes, los bancos proceden a revisar algún tipo de identificación vigente expedida por el gobierno. Esta identificación debe incluir evidencia de la nacionalidad o residencia del cliente e

incluir una fotografía u otra salvaguarda similar. Entre los posibles ejemplos de la misma están la licencia de conducción y el pasaporte. Sin embargo, pueden usarse otros tipos de identificación si éstas le permiten al banco creer razonablemente que conoce la verdadera identidad del cliente. Sin embargo, debido a la existencia de documentos falsos o documentos obtenidos de manera

[38] Para una persona natural: dirección (debe ser de una calle [y no, por ejemplo, un número de casilla postal o Apartado Aéreo]) de la residencia o sitio de negocios, o si la persona no cuenta con dicha dirección, el número de la casilla de correos de Correos del Ejército [Army Post Office – APO] o Correos de Flota [Fleet Post Office – FPO], la dirección (debe ser una calle) de la residencia o negocio del familiar más cercano o de otra persona de contacto, o una descripción de las instalaciones físicas del cliente. Para las personas que no son individuales (tales como las corporaciones, asociaciones o fiducias):, oficina local u otra ubicación física.

[39] El número de identificación para las personas de los Estados Unidos es el de Número de Identificación Tributaria (TIN, por su sigla en inglés) (o la constancia de haberlo solicitado), y para personas que no son de Estados Unidos, uno o más de los siguientes: el NIT (Número de Identificación Tributaria – TIN en inglés); número de pasaporte y país que lo expidió; número de tarjeta de identificación como extranjero; o número y país de expedición de cualquier otro documento vigente expedido por el Gobierno que indique la nacionalidad o residencia y lleve una fotografía u otra salvaguardia similar. El NIT (TIN en inglés) está definido en la sección 6109 del Código de Ingresos Nacionales [Internal Revenue Code] de 1986 (26 USC 6109) y las regulaciones del IRS que implementan dicha sección (por ejemplo, el número del Seguro Social o el número de identificación de empleado).

Para personas no naturales (tales como corporaciones, asociaciones o fiducias), los bancos deben obtener documentos que demuestren la existencia legal de la entidad, tales como certificado de constitución, licencia comercial vigente expedida por el gobierno, contrato de asociación o instrumento fiduciario.

Verificación mediante métodos no documentales

Los bancos no están obligados a emplear métodos no documentales para verificar la identidad de los clientes. Sin embargo, los bancos que emplean métodos no documentales para realizar dicha verificación deben contar con procedimientos que indiquen cuáles son los métodos que emplea el banco para ese fin. Los métodos no documentales pueden incluir el contacto con el cliente; verificación independiente de la identidad del cliente a través de una comparación de información suministrada por el cliente con la información obtenida por una agencia crediticia, base de datos pública u otra fuente; verificación de referencias con otras entidades financieras; y obtención de estados financieros.

Los procedimientos no documentales del banco también deben tratar las siguientes situaciones: una persona natural que no presenta documento de identificación vigente expedido por el gobierno con fotografía hubo otra salvaguarda similar; el banco desconoce los documentos presentados; la cuenta se abre sin obtener documentos (por ejemplo, el banco obtiene la información requerida de parte del cliente, con la intención de verificarla); el cliente abre la cuenta sin comparecer personalmente; o de alguna otra forma se presentan circunstancias que incrementan el riesgo de que el banco no pueda verificar la verdadera identidad de un cliente a través de los documentos de identificación del mismo.

Verificación adicional para ciertos clientes

El CIP debe contemplar casos en los que, con base en su propia evaluación del riesgo que implica una nueva cuenta abierta por un cliente que no es persona natural, el banco podrá obtener información sobre personas naturales que disponen de autoridad o ejercen control sobre dichas cuentas, incluyendo a signatarios, para poder verificar la identidad del cliente. Este método de verificación aplica únicamente cuando el banco no puede verificar la verdadera identidad del cliente a través de métodos documentales o no documentales. Por ejemplo, es posible que un banco requiera obtener información sobre la identidad de un propietario único o de los socios principales en una sociedad, y verificar dicha identidad, cuando de otra forma el banco no puede identificar satisfactoriamente al propietario único o a la sociedad.

Falta de verificación

El CIP también debe contar con procedimientos para circunstancias en las cuales el banco no puede generar la creencia razonable de conocer la verdadera identidad del cliente. Estos procedimientos deben describir lo siguiente:

. • Las circunstancias en las cuales el banco no debe abrir una cuenta
. • Los términos bajo los cuales el cliente podrá utilizar la cuenta mientras que el banco procura verificar la identificación del cliente
. • Las circunstancias en las cuales el banco debe cerrar una cuenta, si fallan los esfuerzos realizados para verificar la identidad del cliente
. • El momento en que el banco debe radicar un ROS de conformidad con las leyes y la regulación aplicables.

REQUISITOS DE REGISTRO Y RETENCIÓN DE DATOS

El CIP de los bancos debe incluir procedimientos para llevar registros. Como mínimo, los bancos deben guardar la información de identificación (nombre, dirección, fecha de nacimiento para personas naturales, NIT [Taxpayer Identification Number – TIN] y cualquier otra información que requiera el CIP) obtenida en el momento de la apertura de la cuenta, durante un período de cinco (5) años después de haberse cerrado esta última[40]. Para las tarjetas de crédito, el período de retención es de cinco (5) años después del cierre de la cuenta o inactividad de la misma.

Los bancos también deben mantener una descripción de los siguientes elementos durante los cinco (5) años siguientes a la creación del respectivo registro:

. • Todo documento empleado para verificar la identidad, observando el tipo de documento, número de identificación, lugar de expedición del mismo y si aplica, fecha de expedición y de expiración.

. • El método utilizado y los resultados obtenidos a partir de medidas tomadas para verificar la identidad.
. • Los resultados de cualquier discrepancia sustancial descubierta al verificar la identidad.

COMPARACIÓN CON LAS LISTAS DEL GOBIERNO

El CIP debe incluir procedimientos para determinar si el cliente aparece en las listas emitidas por el gobierno federal de terroristas u organizaciones terroristas conocidas o sospechosas de serlo[41]. El Departamento del Tesoro de Estados Unidos se comunicará con los bancos, en consulta con las agencias bancarias federales de los mismos, cada vez que se expida una lista. En ese momento los bancos deben comparar sus listas de clientes con los nombres que aparecen en la lista del gobierno, dentro de un plazo razonable después de la apertura de la cuenta o antes de la misma, si lo solicita el gobierno, y seguir las instrucciones que acompañan a la lista.

NOTIFICACIÓN ADECUADA A LOS CLIENTES

[40] Los bancos no están obligados a fotocopiar y retener las fotocopias de los documentos utilizados en el proceso de verificación. Sin embargo, si el banco decide hacerlo, debe asegurarse de guardar muy bien físicamente dichas fotocopias, para protegerse adecuadamente contra el hurto de identidad. Además, esas fotocopias no se deben mantener en el mismo lugar en que están los archivos y la documentación relativa a decisiones crediticias adoptadas, para evitar cualquier problema relacionado con las normas sobre el cumplimiento con los consumidores.

[41] Para la fecha de publicación de este manual, no existen listas oficiales de verificación designadas para los fines del Programa de identificación del cliente (CIP por su sigla en inglés). La comparación de clientes con las listas que requiere la OFAC y los requerimientos de la sección 314(a) (31 CFR 103.100) de la Ley Patriota conduce a que se trata de requerimientos distintos y separados.

El CIP debe incluir procedimientos de notificación oportuna al cliente para informarle que el banco está solicitando información para verificar su identidad. Dicha notificación debe describir en términos generales los requisitos de identificación fijados por el banco y debe suministrarse de manera que se le permita al cliente de manera razonable verla, o de otra forma recibir la notificación, antes de abrir la cuenta. Ejemplos de ello pueden ser la publicación de la notificación en el vestíbulo del banco, o en un sitio web, o en los documentos de solicitud de préstamo. Se ofrece un ejemplo de dicho texto en la siguiente reglamentación:

> INFORMACIÓN IMPORTANTE SOBRE LOS PROCEDIMIENTOS A SEGUIR PARA LA APERTURA DE CUENTAS -Para colaborar con el gobierno federal en la lucha contra la financiación del terrorismo y el lavado de dinero, la leyes federales requieren que toda entidad financiera obtenga, verifique y registre información que permita identificar a todo quien abra una cuenta. Para Ud(s). esto implica lo siguiente: al abrir su cuenta, solicitaremos su nombre, dirección, fecha de nacimiento y otra información que nos permita identificarlo(a). También podremos solicitarle presentar su licencia de conducción u otros documentos de identificación.

DEPENDENCIA DE OTRAS ENTIDADES FINANCIERAS

Los bancos pueden depender de otras entidades financieras (incluyendo entidades afiliadas) para proceder con la totalidad o parte de los elementos que constituyen el CIP, si dicha dependencia se plantea en el CIP y se cumplen las siguientes condiciones:

- La entidad financiera de la cual se depende está sujeta a una reglamentación final de implementación de los requisitos del programa AML según la 31 USC 5318(h) y está sujeta a regulación por parte de un ente regulador federal funcional[42].
- El cliente tiene una cuenta o está en proceso de abrirla en el banco y también en la otra entidad funcionalmente regulada.
- La dependencia es razonable, bajo las circunstancias.
- La otra entidad financiera celebra un contrato por medio del cual se compromete a certificar anualmente ante el banco que ha implementado su propio programa AML, y que cumplirá (o que su agente cumplirá) con los requisitos especificados relativos al CIP del banco.

La reglamentación definitiva no altera la autoridad del banco para emplear a terceros, tales como un agente o proveedor de servicios, para que lleven a cabo dichas funciones en su nombre. Por lo tanto, el banco podrá hacer arreglos con terceros, tales como concesionarios de automóviles o intermediarios hipotecarios, para que actúen como sus agentes respecto a un préstamo, para verificar la identidad de sus clientes. El banco también podrá hacer arreglos con terceros respecto a los registros de datos respectivos. Sin embargo, al igual que con cualquier otra responsabilidad a cargo de terceros, es el banco quien detenta la responsabilidad última del cumplimiento de dichos terceros con

[42] Regulador federal funcional significa lo siguiente: Junta de Gobernadores del Sistema de la Reserva Federal; Corporación Federal de Seguros de Depósitos; Administración Nacional de Cooperativas de Crédito; Oficina del Contralor de la Moneda; Oficina de Supervisión de Entidades de Ahorro y Crédito; Comisión de Vigilancia y Control del Mercado de Valores [Securities and Exchange Commission]; o Comisión de Comercio en Futuros de Bienes Básicos [Commodity Futures Trading Commission].

los requerimientos del CIP del banco. Como resultado de ello, los bancos deben establecer controles adecuados y procedimientos de revisión respecto a dichas relaciones. Este requisito contrasta con la disposición de dependencia de la reglamentación, la cual permite que la parte en la cual se depende asuma dicha responsabilidad.

OTROS REQUISITOS LEGALES

Ninguna regla contenida en el CIP exime al banco de sus obligaciones bajo las disposiciones de las leyes, reglas y reglamentaciones BSA y AML, particularmente en lo relacionado con las que indican cuál es la información que se debe obtener, verificar o mantener respecto a toda cuenta o transacción realizada.

La Tesorería de los Estados Unidos y las agencias bancarias federales le han suministrado a los bancos Preguntas frecuentes (FAQ – Frequently Asked Questions), las cuales se revisan

periódicamente. Dichas Preguntas frecuentes y otros documentos relacionados (por ejemplo las reglas CIP) están disponibles en los sitios web de FinCEN y de las agencias bancarias federales.

Visión general fundamental – Debida diligencia del cliente

OBJETIVO

Evaluar si son apropiadas y completas las políticas, procedimientos y procesos de debida diligencia del cliente (CDD) empleados por el banco para obtener información sobre los clientes, y evaluar la utilidad de dicha información para detectar, monitorear y reportar actividades sospechosas.

VISIÓN GENERAL

La piedra angular de todo buen programa de cumplimiento BSA/AML es la adopción e implementación de políticas, procedimientos y procesos CDD (debida diligencia del cliente) para todos los clientes, especialmente los que presentan un alto riesgo de lavado de dinero y financiación del terrorismo. El objetivo de los procedimientos de debida diligencia del cliente debe ser permitirle al banco predecir con relativa certeza los tipos de transacciones que probablemente habrá de realizar un cliente. Estos procedimientos ayudan al banco a determinar en qué momento pueden ser potencialmente sospechosas estas transacciones. El concepto de la debida diligencia del cliente comienza con la verificación de la identidad de los mismos y la evaluación de los riesgos que implican. Los procedimientos también deben incluir una debida diligencia del cliente mejorada o realzada para clientes de alto riesgo, así como una debida diligencia continua aplicada a la base de clientes actuales.

Las políticas, procedimientos y procesos eficaces de debida diligencia de clientes aportan un marco esencial que le permite al banco cumplir con los requisitos regulatorios y reportar operaciones sospechosas. Un ejemplo de este concepto se ofrece en el Apéndice K ("Riesgo del cliente versus debida diligencia y monitoreo de operaciones sospechosas"). Las políticas, procedimientos y procesos de debida diligencia del cliente son clave para el banco porque contribuyen a lo siguiente:

. • Detectar y reportar transacciones inusuales o sospechosas que tienen el potencial de exponer al banco a pérdidas financieras, mayores gastos o afectar su reputación.
. • Evitar la exposición del banco a personas que utilizan o procuran utilizar los productos y servicios del banco con fines ilícitos.
. • Adherirse a las prácticas bancarias seguras y sólidas.

GUÍA PARA LA DEBIDA DILIGENCIA DEL CLIENTE

Las políticas, procedimientos y procesos BSA/AML deben incluir pautas o guías para la debida diligencia del cliente (CDD) que cumplan con las siguientes condiciones:

. • Corresponder al perfil de riesgo BSA/AML del banco, especialmente con respecto a clientes de alto riesgo.
. • Incluir una declaración clara sobre las expectativas generales de la gerencia y fijar responsabilidades concretas al personal, incluyendo a la persona encargada de revisar y aprobar cambios en la calificación o perfil de riesgo de los clientes, según aplique.
. • Asegurarse de que el banco cuente con suficiente información sobre los clientes como para implementar un sistema eficaz de monitoreo de operaciones sospechosas.
. • Suministrar orientación para la documentación del análisis que hace parte del proceso de debida diligencia, incluyendo orientación para la resolución de casos en que no se cuente con suficiente información o ésta sea incorrecta o imprecisa.
. • Asegurarse de que el banco disponga de información actualizada de sus clientes.

RIESGO QUE IMPLICAN LOS CLIENTES

La gerencia debe entender muy bien cuál es el riesgo de lavado de dinero o financiación del terrorismo que implica la base de clientes del banco. Bajo este enfoque, el banco debe obtener suficiente información al momento de abrir una cuenta como para desarrollar un buen nivel de conocimientos sobre las actividades corrientes que se pueden esperar de parte de ese cliente, según la ocupación u operaciones de negocios de cada cliente.

Mucha de la información CDD se puede confirmar a través de agencias que reportan datos, las referencias bancarias (para las cuentas grandes), correspondencia y conversaciones telefónicas con los clientes y visitas a los lugares de negocios de los mismos. Algunas medidas adicionales pueden incluir el uso de referencias de terceros o la investigación de información que está disponible a nivel público (por ejemplo, a través de Internet o bases de datos comerciales).

Los procedimientos CDD deben incluir un monitoreo periódico de la relación con el cliente para determinar si se han presentado cambios importantes en la información CDD original (por ejemplo, cambios en el empleo u operaciones de negocios).

Debida diligencia mejorada para clientes de alto riesgo

Los clientes que representan un alto riesgo de lavado de dinero o financiación del terrorismo incrementan el grado de exposición del banco y por lo tanto se deben aplicar políticas, procedimientos y procesos de debida diligencia especiales. Es fundamental aplicar una debida diligencia especial a los clientes de alto riesgo para poder entender sus posibles transacciones por anticipado e implementar un sistema de monitoreo de actividades sospechosas que permita reducir riesgos que puedan afectar la reputación, el cumplimiento y las transacciones del banco. Los clientes de alto riesgo y sus transacciones se deben revisar más de cerca en el momento de apertura de cuentas, así como con mayor frecuencia durante el transcurso de su relación con el banco. En la página 17 de la sección de revisión general fundamental titulada "Diseño del alcance y la planeación" el lector podrá encontrar una guía para la identificación de los clientes de alto riesgo.

Un banco puede decidir que un cliente representa un alto riesgo debido a la actividad comercial del mismo o la estructura de sus propiedades, el tipo y volumen de sus transacciones realizadas o planeadas, incluyendo aquellas relacionadas con jurisdicciones de alto riesgo. Si es así, el banco debe considerar la posibilidad de obtener, tanto en el momento de la apertura de la cuenta como durante el transcurso de la relación con el cliente, la siguiente información sobre el mismo:

. • propósito de la cuenta • origen de los fondos y de la riqueza

. • propietario beneficiario de las cuentas, si aplica • ocupación o tipo de negocios del cliente (o propietario beneficiario)

. • estados financieros

. • referencias bancarias

. • domicilio (localidad en donde se constituyó el negocio)

. • proximidad de la residencia, lugar de empleo o sede de negocios del cliente con respecto al banco

. • descripción de la zona de actividad comercial principal del cliente, e información sobre si éste efectuará transacciones internacionales de manera habitual

. • descripción de las operaciones de negocios, volumen anticipado de moneda y ventas totales, y lista de los principales clientes y proveedores

. • explicación de cambios efectuados en las actividades de las cuentas

Visión general fundamental – Reportes sobre operaciones sospechosas (ROS)

OBJETIVO

Evaluar las políticas, procedimientos y procesos del banco y el cumplimiento general del mismo con los requisitos estatutarios y regulatorios para el monitoreo, la detección y la elaboración de informes sobre operaciones sospechosas.

VISIÓN GENERAL

Los formularios empleados para reportar actividades sospechosas constituyen la piedra angular del sistema de informes de la Ley del Secreto Bancario. Se trata de algo fundamental para la capacidad de los Estados Unidos de emplear información financiera para combatir el terrorismo, la financiación del terrorismo, el lavado de dinero y otros delitos financieros. Dentro de este sistema, FinCEN y las agencias bancarias federales reconocen que, desde una perspectiva práctica, no es posible que los bancos detecten y reporten todas las actividades potencialmente ilícitas que fluyen por el banco. Los examinadores se deben enfocar en la evaluación de las políticas, procedimientos y procesos del banco que permitan identificar e investigar operaciones sospechosas. Sin embargo, como parte del proceso de examen, los examinadores deben revisar las decisiones de elaboración y radicación de Informes de operaciones sospechosas (ROS) del banco para determinar la eficacia de los procesos de monitoreo y producción de informes sobre las mismas. Por encima de todo, los examinadores y los bancos deben reconocer que la calidad de los datos ROS es de máxima importancia para una implementación efectiva del sistema

de informes de operaciones sospechosas.

Los bancos, las corporaciones *holding* [propietarias o controladoras] de bancos y las subsidiarias de las mismas están obligadas por regulación federal[43] a radicar un ROS en los siguientes casos:

. • violaciones criminales que incluyan abuso por parte de personal interno, por cualquier monto;
. • violaciones criminales por un monto de US $ 5.000 o más, cuando es posible identificar a un sospechoso;
. • violaciones criminales por un monto de US $25.000 o más, no importa cuál sea el sospechoso potencial;
. • transacciones realizadas por, en o a través del banco (o una subsidiaria), o el intento de realizarlas, por un monto de US $ 5.000 o más, siempre que el banco o la subsidiaria sepan, sospechen o tengan fundamento para sospechar que dichas transacciones:

[43] Ver CFR 208.62, 211.5(k), 211.24(f) y 225.4(f) (Junta de Gobernadores del Sistema de la Reserva Federal); 12 CFR 353 (Corporación Federal de Seguros de Depósitos); 12 CFR 748 (Administración Nacional de Cooperativas de Crédito); 12 CFR 21.11 (Oficina del Contralor de la Moneda); 12 CFR 563.180 (Oficina de Supervisión de Entidades de Ahorro y Crédito); (no aplica para las empresas *holding* o propietarias de las Corporaciones Ahorro y Crédito); y 31 CFR 103.18 (FinCEN).

– pueden incluir la posibilidad de lavado de dinero u otras actividades ilícitas (por ejemplo, financiación del terrorismo) – están diseñadas para evadir la Ley del Secreto Bancario o la reglamentación efectiva de la misma – no presentan finalidad comercial o ilícita y no constituyen el tipo de transacción que se esperaría del cliente particular en cuestión, y el banco no cuenta con una explicación razonable que justifique dicha transacción luego de examinar los datos y hechos disponibles, incluyendo los antecedentes y la posible finalidad de la transacción.

Las transacciones pueden incluir depósitos; retiros; transferencias entre cuentas; intercambios de moneda; ampliación de créditos; compra o venta de acciones, bonos, certificados de depósito u otros instrumentos monetarios o títulos valores de inversión; o cualesquiera otros pagos, transferencias o entregas realizadas por un banco o a través del mismo o con destino al mismo.

Protección ('Puerto Seguro') bancaria por responsabilidad civil por los Reportes de operaciones sospechosas (ROS) [SAR – Suspicious Activity Report]

La ley Federal (31 USC 5318 (g)(3)) protege contra la responsabilidad civil derivada de los Reportes de operaciones sospechosas (ROS) entregados a las autoridades respectivas, incluyendo toda la documentación de soporte, sin importar si dichos informes han sido radicados o no de conformidad con las instrucciones ROS. Concretamente, la ley dispone que los bancos y sus directivos, funcionarios, empleados y agentes que divulguen información a las autoridades sobre posibles violaciones de la ley o de las regulaciones, incluyendo información relacionada con la elaboración de los informes ROS, "no serán

responsables ante persona alguna bajo ley o reglamentación alguna de los Estados Unidos o constitución, ley o regulación de Estado alguno [de los Estados Unidos] o subdivisión político-administrativa alguna de Estado alguno [de los Estados Unidos], o bajo contrato u otro pacto alguno que se pueda hacer valer legalmente (incluyendo pactos de arbitramiento) en razón de dicha divulgación o por no haber notificado sobre la misma a la persona objeto de la divulgación o a cualquier otra persona identificada en la divulgación". Esta medida de protección o "puerto seguro" aplica para los ROS entregados según los parámetros fijados para la elaboración de dichos informes así como para los ROS sobre cualquier actividad entregados voluntariamente que estén por debajo del umbral fijado para los mismos.

SISTEMAS PARA IDENTIFICAR, INVESTIGAR Y REPORTAR ACTIVIDADES SOSPECHOSAS

Las políticas, procedimientos y procesos deben indicar quienes son las personas responsables de la identificación, investigación y elaboración de los Informes de operaciones sospechosas. Deben existir políticas, procedimientos y procesos apropiados para monitorear e identificar actividades inusuales. El nivel del monitoreo lo determina la evaluación de riesgo del propio banco, con énfasis especial en los productos, servicios, clientes y ubicaciones geográficas de alto riesgo. Los sistemas de monitoreo típicamente incluyen identificación de empleados en los casos de remisiones, sistemas manuales, sistemas automatizados o cualquier combinación de los mismos. El banco debe asegurarse de asignar personal adecuado para la identificación, investigación y Cuando se identifican actividades inusuales, típicamente se realiza investigación adicional. La información de Debida diligencia del cliente (CDD) ayuda a los bancos a determinar si alguna actividad inusual puede considerarse como sospechosa (para mayor información, ver la discusión sobre la "Debida diligencia de los clientes" que aparece en la sección de visión general fundamental de la página 37). Luego de una completa investigación y un concienzudo análisis, toda decisión que se tome sobre radicar o no radicar un ROS debe quedar documentada. Si aplica, la revisión y comprensión del monitoreo de actividades sospechosas en la totalidad de las subsidiarias, líneas de negocio y tipos de riesgo de la organización (por ejemplo, reputación, cumplimiento o transacción) pueden mejorar la capacidad de la organización bancaria de detectar actividades sospechosas y así minimizar las posibilidades de pérdidas financieras, mayores gastos y puesta en riesgo de la reputación de la misma. Ver la sección de visión general ampliada titulada "Programa de cumplimiento BSA/AML empresarial integral" de la página 93 para una mayor información.

Monitoreo manual de transacciones

Los sistemas manuales de monitoreo de transacciones consisten en la revisión de los distintos informes que generan los sistemas de gestión de información (MIS – Management Information Systems) del banco o de los distribuidores o fabricantes de los mismos. Algunos sistemas MIS bancarios emplean como complemento sistemas de distribuidores o fabricantes diseñados para identificar transacciones en moneda que son reportables y llevar registros obligatorios de transferencias de fondos. Muchos de estos sistemas de

distribuidores o fabricantes incluyen modelos de filtración para identificar actividades inusuales. Entre los ejemplos de los informes MIS están los informes de actividades monetarias, transferencias de fondos, ventas de instrumentos monetarios, reportes de grandes volúmenes, informes de cambios significativos en saldos e informes sobre fondos insuficientes (NSF). El tipo y la frecuencia de las revisiones realizadas y los respectivos informes empleados deben corresponder al perfil de riesgo BSA/AML del banco y cubrir adecuadamente sus productos, servicios, clientes y ubicaciones geográficas de alto riesgo.

Los informes producidos por los sistemas MIS del banco o de distribuidores o fabricantes típicamente emplean un umbral en dólares fijado a discreción. Los umbrales seleccionados por la gerencia para la elaboración de informes de transacciones deben permitirle a ésta detectar actividades inusuales. Si se identifica una actividad inusual, el personal encargado deberá revisar la información CDD y cualquier otra información relevante para determinar si la actividad es sospechosa. La gerencia debe evaluar periódicamente la utilidad y validez de los criterios de filtración y los umbrales empleados en el proceso de monitoreo. Cada banco debe evaluar e identificar los criterios de filtración que sean más apropiados para la entidad respectiva. A continuación se presenta una descripción de los informes típicos de monitoreo de transacciones manuales. Además, es necesario revisar qué tan razonables son los criterios de filtración empleados en la programación de los sistemas de monitoreo del banco.

Informes de actividades en moneda [Currency Activity Reports]: La mayoría de los distribuidores y fabricantes ofrecen informes que identifican todas las actividades realizadas en moneda, o todas las actividades realizadas en moneda por encima de los US $ 10.000. Estos informes ayudan a los banqueros a radicar los Informes de transacciones en moneda (CTR – Currency Transaction Reports) y a identificar operaciones sospechosas. La mayoría de los proveedores de servicios de información bancaria ofrecen informes de actividades en moneda capaces de filtrar transacciones según una variedad de parámetros, como por ejemplo los siguientes:

. • Actividades en moneda incluyendo transacciones múltiples por un valor superior a US $ 10.000.
. • Actividades en moneda (transacciones sencillas y múltiples) por un valor inferior al requerimiento fijado para la elaboración de informes (es decir, entre US $ 7.000 y $ 10.000).
. • Transacciones en moneda en múltiples transacciones en dólares por montos más bajos (por ejemplo, US $ 3.000) que generan una suma sustancial al cabo de un tiempo (por ejemplo, US $ 30.000 al cabo de 15 días).

Registros de transferencias de fondos [Funds Transfer Records]: La Ley del Secreto Bancario exige que los bancos registren las transferencias de fondos cuyo valor sea igual o superior a US $ 3.000. La revisión periódica de esta información puede ayudar a los bancos a identificar patrones de actividades inusuales. Esta revisión periódica de registros de transferencias de fondos realizadas en bancos con bajos volúmenes de transferencias generalmente basta para identificar actividades inusuales. Para los bancos con mayores volúmenes de transferencias, el empleo de hojas de cálculo o software de distribuidores o fabricantes constituye una manera eficiente de revisar las transferencias de fondos para detectar patrones inusuales. La mayoría de los sistemas de software de distribuidores o

fabricantes incluye informes estándares con filtros que aplican para las operaciones sospechosas. Estos informes típicamente se enfocan en la identificación de algunas ubicaciones geográficas de alto riesgo y transferencias de fondos en dólares realizadas por personas y empresas. En la búsqueda de actividades inusuales también deben revisarse las transferencias de fondos realizadas por quienes no son clientes del banco, así como las transacciones pagaderas mediante identificación apropiada (PUPID
– Payable Upon Proper Identification).

Registros de Instrumentos Monetarios [Monetary Instrument Records]: La Ley del Secreto Bancario [BSA] exige a los bancos llevar registros de las ventas de instrumentos monetarios. Estos registros pueden ayudar al banco a identificar la posible estructuración de moneda a través de la compra de cheques de gerencia, cheques oficiales, giros postales o cheques viajeros por valores entre US $ 3.000 y US $ 10.000. Una revisión periódica de estos registros también puede ayudar a identificar compras frecuentes de instrumentos monetarios y destinatarios y beneficiarios frecuentes.

Monitoreo automatizado de cuentas

Los sistemas automatizados de monitoreo de cuentas típicamente emplean programas de computación desarrollados internamente o adquiridos de fabricantes o distribuidores, para identificar transacciones individuales, patrones de actividades inusuales o cualquier desviación con respecto a las actividades esperadas. Estos sistemas pueden capturar una amplia gama de actividades de cuentas, tales como depósitos, retiros, transferencias de fondos, transacciones automatizadas de cámara de compensación (ACH – automated clearing house transactions) y transacciones automatizadas de cajeros electrónicos (ATM), directamente a partir del sistema de procesamiento central de datos del banco. Los bancos grandes que operan en muchas localidades o que tienen un gran número de clientes de alto riesgo típicamente emplean sistemas automatizados de monitoreo de cuentas.

Los actuales sistemas automatizados incluyen sistemas que se basan en reglas y sistemas inteligentes. Los sistemas basados en reglas detectan transacciones inusuales que caen por fuera de las "reglas" que desarrolla el mismo sistema o define la gerencia. Estos sistemas pueden manejar muy pocas o muchas reglas, dependiendo de la complejidad del programa de software desarrollado internamente o adquirido de un distribuidor o fabricante. Las reglas se aplican mediante una serie filtros de transacciones o mediante un motor de reglas [rules engine]. Los sistemas automatizados basados en reglas son más sofisticados que el sistema básico manual, el cual únicamente filtra una sola regla (por ejemplo, todas las transacciones cuyo volumen sea superior a US $ 10.000). Los sistemas de monitoreo automatizados basados en reglas pueden aplicar múltiples filtros complejos. Por ejemplo, pueden aplicar filtros primero a la totalidad de las cuentas, y luego a un subconjunto de cuentas
o a una categoría particular de riesgo (como por ejemplo, todos los clientes que cuenten con consignación directa [direct deposit] o todos los clientes que sean restaurantes). Los sistemas de monitoreo basados en reglas también pueden filtrar perfiles individuales de cuentas de clientes.

Los sistemas inteligentes tienen la capacidad de adaptarse y modificar así sus análisis con el tiempo, sobre la base de patrones de actividad, tendencias recientes, cambios en la base de clientes y otros datos relevantes. Los sistemas inteligentes revisan las transacciones en el contexto de otras transacciones y del perfil del cliente. Al hacerlo, aumenta la información que incluyen en su base de datos sobre clientes, tipos de cuentas, categorías o negocios, a medida que ingresan y se almacenan más transacciones y más datos en el sistema.

Entender los criterios de filtración que emplean los sistemas de monitoreo basados en software es clave para entender la efectividad de los sistemas automatizados de monitoreo de cuentas. Los criterios de filtración se deben desarrollar con base en una revisión concreta de los clientes, los productos y los servicios de alto riesgo. Dichos criterios de filtración, incluyendo perfiles y reglas específicas, deben fundamentarse en lo que sea razonable y lo que cabe esperar según cada tipo de cliente. Llevar a cabo un monitoreo de clientes únicamente basado en las actividades históricas de los mismos puede prestarse para equivocaciones, si las actividades no concuerdan con tipos similares de clientes. Por ejemplo, es posible que un cliente presente un historial de transacciones sustancialmente distinto a lo que se podría esperar normalmente de ese tipo de cliente (concretamente, un negocio de cambio de cheques que deposite grandes sumas de dinero, versus retiros de dinero efectuados para financiar el pago de cheques con efectivo).

La autoridad para fijar o modificar perfiles de actividad esperados debe estar claramente definida y generalmente requerir la aprobación del oficial de cumplimiento con la Ley del Secreto Bancario o de la alta gerencia. Se debe restringir el acceso al sistema de monitoreo mediante controles. La gerencia debe documentar o ser capaz de explicar los criterios de filtración y los umbrales utilizados, así como por qué éstos corresponden a los riesgos que enfrenta el banco. La gerencia también debe revisar periódicamente los criterios de filtración y los umbrales establecidos, para asegurar la eficacia de los mismos. Además, la metodología de programación empleada por el banco debe ser validada por terceros independientes.

Identificación de los delitos subyacentes

Los bancos están obligados a reportar operaciones sospechosas que pueden incluir lavado de dinero, violaciones de la Ley del Secreto Bancario, financiación del terrorismo[44] y otros delitos que sobrepasan los umbrales respectivos fijados en dólares. Sin embargo, los bancos no están obligados a investigar ni confirmar los posibles delitos resultantes (por ejemplo, financiación del terrorismo, lavado de dinero, evasión tributaria, hurto de identidad, y varios tipos de fraudes). La respectiva investigación es responsabilidad de las autoridades. [Pero] Al evaluar las operaciones sospechosas y diligenciar sus ROS, los bancos sí deben identificar las características de las operaciones sospechosas al máximo grado posible. La sección 35 de la Parte III de los ROS presenta 20 características distintas de operaciones sospechosas. Aunque existe una categoría titulada "Otros", ésta debe utilizarse únicamente cuando no sea posible identificar una situación con las 20 categorías suministradas.

Averiguaciones y consultas policiales

Los bancos deben establecer políticas, procedimientos y procesos para identificar a quienes sean objeto de solicitudes policiales, vigilar o monitorear las transacciones de dichas personas, identificar operaciones inusuales o sospechosas asociadas a dichas personas, y elaborar y radicar ROS relativos a dichas personas, según corresponda. Las consultas o averiguaciones y solicitudes formuladas por las autoridades pueden incluir citaciones penales, cartas de seguridad nacional (NSL – national security letters) y solicitudes de la sección 314 (a).

El solo hecho de recibir una solicitud o una averiguación policial no obliga al banco a elaborar y radicar un ROS [Reporte de operaciones sospechosas]. Sin embargo, es posible que las solicitudes formuladas por las autoridades sean relevantes para la evaluación general que hace el banco del riesgo que representan sus propios clientes y sus cuentas. Es responsabilidad del banco evaluar toda la información que conozca sobre sus clientes, incluyendo la posibilidad de recibir solicitudes policiales, de conformidad con su programa de cumplimiento BSA/AML basado en riesgo. El mismo banco es quien determina si debe radicar un ROS con base en toda la información que conoce de sus clientes.

Cartas de seguridad nacional (NSL – National Security Letters)

[44] Es si un banco conoce o sospecha o tiene razones para sospechar que un cliente puede estar vinculado a actividades terroristas en contra de los Estados Unidos, debe llamar inmediatamente al teléfono gratuito de Emergencias terroristas para entidades financieras [Financial Institutions Terrorist Hotline] de FinCEN: 1-866-556-3974. De la misma manera, si cualquier otro tipo de sospecha de violación requiere atención inmediata, como por ejemplo una operación de lavado de dinero que está en curso, el banco debe notificar a las agencias bancarias federales y autoridades respectivas. En cualquier caso el banco también debe radicar un ROS.

Las NSL son requerimientos de investigación que expiden la FBI (Oficina Federal de Investigaciones) y otras autoridades gubernamentales federales [de EE. UU.] en el transcurso de investigaciones de contrainteligencia y lucha contra el terrorismo, con el objetivo de obtener lo siguiente:

. • registros de comunicaciones telefónicas y electrónicas provenientes de las empresas telefónicas y los proveedores de servicios de Internet[45];
. • información proveniente de las agencias de calificación de crédito[46];
. • registros financieros de las entidades financieras[47].

Las NSL son altamente confidenciales[48]. Según 12 USC 3414(a)(3) y (5)(D), ningún banco ni funcionario o empleado o agente bancario puede revelarle a persona alguna que una autoridad gubernamental o el FBI ha(n) solicitado o ha(n) logrado acceder a los registros a través de una NSL bajo la Ley del Derecho a la Privacidad Financiera [Right to Financial Privacy Act]. Los bancos que reciben NSL deben tomar medidas apropiadas para asegurar la confidencialidad de dichas cartas, y deben establecer procedimientos para su procesamiento y para mantener la confidencialidad de las mismas.

Si un banco elabora y radica un informe ROS luego de haber recibido una NSL, dicho informe no debe incluir referencia alguna al recibo de la NSL ni a la existencia de la misma. El informe ROS debe referirse únicamente a los hechos y actividades que permitan sustentar que el banco ha identificado transacciones inusuales o sospechosas.

Toda pregunta relativas a las NSL debe dirigirse a la oficina de terreno de la FBI del banco local. En la dirección de Internet www.fbi.gov se puede encontrar información para comunicarse con las oficinas de terreno de la FBI.

PROCESO DE TOMA DE DECISIONES ROS

El banco debe contar con políticas, procedimientos y procesos para remitir actividades inusuales provenientes de todas las líneas de negocios al personal o al departamento encargado de evaluarlas. Este proceso debe asegurar que toda la información aplicable (por ejemplo, citaciones penales, NSL o solicitudes de la Sección 314(a)) sean efectivamente evaluadas.

Es altamente deseable que los bancos documenten sus decisiones sobre los Informes de operaciones sospechosas (ROS). La decisión de elaborar y radicar un informe ROS constituye una decisión inherentemente subjetiva. Los examinadores deben fijarse si el banco cuenta con un proceso eficaz de toma de decisiones sobre los ROS, y no en casos

[45] Ley sobre la Privacidad en las Comunicaciones Electrónicas [Electronic Communications Privacy Act], 18 USC 2709.

[46] Ley sobre Informes de Crédito Justos [Fair Credit Reporting Act], 15 USC 1681u

[47] Ley del Derecho a la Privacidad Financiera de 1978 [Right to Financial Privacy Act], 12 USC 3401 *et seq*.

[48] Ver la publicación *SAR Activity Review* [Revista de actividades relativas a los ROS], volumen 8 de abril de 2005, para conocer mayor información sobre las Cartas de seguridad nacional [NSL] disponible en www.fincen.gov.

concretos de decisiones sobre dichos informes. Es posible que los examinadores revisen decisiones concretas tomadas sobre los informes ROS para evaluar la eficacia del proceso de monitoreo, elaboración de informes y toma de decisiones sobre los ROS. Cuando un banco cuenta con un proceso de toma de decisiones sobre dichos informes, cumple con las políticas, procedimientos y procesos establecidos para ellos y llega a una decisión de no radicar un informe ROS, no se debe criticar al banco por no haber entregado dicho informe, a menos que sea evidente la existencia de alguna falla o de mala fe.

MOMENTO OPORTUNO PARA LA RADICACIÓN DE UN REPORTE DE OPERACIONES SOSPECHOSAS (ROS) [SAR – Suspicious Activity Report]

Las reglas sobre los Reportes de Operaciones Sospechosas (ROS) establecen que éstos se

deben radicar como máximo treinta (30) días calendario después de la fecha de la detección inicial de una actividad sospechosa, salvo si no es posible identificar a sospechoso alguno. En ese caso, el período fijado para la radicación de un ROS se extiende a sesenta (60) días. Es posible que las organizaciones tengan que revisar las transacciones o cuentas de un cliente para determinar si deben elaborar y radicar un ROS. La necesidad de revisar las actividades o transacciones de un cliente no necesariamente significa que hay que radicar un ROS. El tiempo disponible para la radicación de estos informes se inicia cuando, durante el transcurso de su revisión o debido a otros factores, la organización descubre o sospecha que las actividades o transacciones que están siendo revisadas corresponden a una o más de las definiciones de operaciones sospechosas[49].

Siempre que ello sea posible, se recomienda hacer una revisión expedita de la transacción o de la cuenta en cuestión. Dicha revisión puede representar una colaboración significativa para las autoridades. En todo caso, se debe completar la revisión en un período de tiempo razonable. Para las violaciones que requieren atención inmediata, tales como las que están en curso, los bancos deben notificar de inmediato, por vía telefónica, a una "autoridad apropiada" y también, según sea necesario, al ente regulador primario del banco, además de elaborar y radicar oportunamente un informe ROS. En términos generales, una "autoridad apropiada" consiste en la División de Investigaciones Penales del Servicio de Ingresos Nacionales (IRS – Internal Revenue Service) o el FBI. El hecho de notificar a las autoridades respecto a operaciones sospechosas no exonera a los bancos de su deber de radicar los informes ROS.

NOTIFICACIÓN A LA JUNTA DIRECTIVA

Las reglas de las agencias bancarias federales sobre informes ROS requieren que los bancos notifiquen a sus juntas directivas o a los comités correspondientes de las mismas cada vez que se radica uno de estos informes[50]. Sin embargo, las reglas no disponen un formato particular para estas notificaciones, y por lo tanto los bancos pueden proceder a estructurar los respectivos formatos con flexibilidad. Los bancos pueden entregar copias de los informes ROS a la junta directiva o a los comités correspondientes de las mismas, pero no están en la obligación de hacerlo. Conversamente, pueden entregar resúmenes, o tablas de informes ROS radicados según tipos concretos de violaciones, u otros tipos de notificaciones. No importa cuál sea el formato empleado para las notificaciones, [en todo caso] la gerencia del banco debe proporcionar suficiente información sobre los informes radicados a la junta directiva o al respectivo comité autorizado de la misma como para cumplir debidamente con sus obligaciones fiduciarias[51].

[49] Grupo de Asesoría de la Ley del Secreto Bancario [Bank Secrecy Act Advisory Group], "Sección 5--Temas y orientación" en *The SAR Activity Review – Trenes, Tips & Issues* [Revista de actividades relativas a los ROS – Tendencias, sugerencias prácticas y temas], octubre de 2000, página 27.

[50] Las cooperativas de ahorro y crédito [credit unions] no están sujetas al requerimiento regulatorio de notificar a las juntas directivas sobre la radicación de informes ROS, aunque muchas proceden con dicha notificación simplemente como una buena práctica.

RADICACIÓN DE INFORMES ROS SOBRE ACTIVIDADES CONTINUADAS

Uno de los propósitos de la radicación de los ROS consiste en identificar violaciones reales o potenciales de la ley ante las autoridades respectivas, para la investigación de las mismas. Este objetivo se cumple cuando los informes radicados identifican las respectivas actividades que suscitan preocupación. Si dichas actividades persisten en el tiempo, se debe informar a las autoridades (así como las agencias bancarias federales). Las pautas fijadas por FinCEN sugieren que los bancos reporten las operaciones sospechosas constantes mediante la radicación de un informe como mínimo cada noventa (90) días[52]. Esta práctica permite notificar a las autoridades sobre el carácter continuo de las actividades en cuestión, y también le recuerda al banco que debe continuar revisando las operaciones sospechosas para decidir si se requiere alguna medida adicional, como por ejemplo una decisión de la gerencia de dar por terminada la relación con el cliente o con el empleado que es objeto del informe.

Los bancos deben desarrollar políticas, procedimientos y procesos para determinar cuándo se requiere escalar los asuntos o problemas identificados como resultado de la radicación repetida de ROS sobre las cuentas. Los procedimientos deben incluir la siguiente:

. • revisión por parte de la alta gerencia y de la oficina jurídica (por ejemplo, el oficial de cumplimiento BSA o el comité sobre los informes ROS)
. • los criterios a emplear cuando se requiere hacer un análisis general de la relación con el cliente
. • los criterios que determinan cuando se debe cerrar una cuenta
. • los criterios que determinan cuando se debe notificar a las autoridades, si corresponde.

[51] Como se observó en el *SAR Activity Review* [Revista de actividades relativas a los ROS], volumen 2 de junio de 2001, "en las raras ocasiones en que la actividad sospechosa está relacionada con alguna persona de la organización, como por ejemplo el presidente o uno de los miembros de la junta directiva, no se debe seguir la política establecida de notificar a dicha persona sobre la radicación de un informe ROS. Toda variación con respecto a las políticas y procedimientos establecidos realizada para evitar el envío de una notificación sobre la radicación de un ROS a la misma persona objeto de dicho ROSS debe quedar documentada, y debe informarse al respecto a todo el personal organizativo de alto nivel no involucrado".

[52] Id [*Nota del Traductor*: Ibid.]
Los informes ROS que deben radicar los bancos deben ser completos, concienzudos y oportunos. En ellos los bancos deben incluir toda la información sospechosa que conozcan. La importancia que tiene la precisión de esta información es muy alta. La falta de precisión en los ROS, así como las narraciones incompletas o desorganizadas, pueden dificultar o imposibilitar su análisis posterior. Sin embargo, hay razones legítimas por las cuales puede ser imposible incluir cierta información en los informes ROS, como por ejemplo cuando no se cuenta con la respectiva información. Incluir una narración concienzuda y completa puede marcar la diferencia, al permitir que las autoridades logren entender claramente cuál es la conducta que se describe y su posible origen criminal. Debido a que la parte de la narración de los informes ROS es la única que resume las operaciones sospechosas, dicho componente de los informes, tal como se menciona en el formulario ROS, es "vital". Por lo

tanto, no describir apropiadamente los factores que convierten en sospechosa a una transacción o actividad menoscaba el propósito de los ROS.

Debido a su naturaleza los ROS son subjetivos, y en general los examinadores no deben criticar la interpretación que haga el banco de los hechos. Sin embargo, los bancos deben procurar que sus narrativas ROS sean completas y concienzudas y describan la extensión y naturaleza de las operaciones sospechosas dentro de los límites que proporciona el ROS (es decir, no se deben incluir anexos en la sección de la narrativa porque no quedarán incluidos en la base de datos de los informes sobre la Ley del Secreto Bancario). El Apéndice L ("Guía de calidad para los ROS") proporciona más orientación a los bancos sobre la redacción de las narrativas ROS y también brinda asistencia a los examinadores al respecto. Además, FinCEN ofrece una orientación integral ("Guía para la elaboración de una narrativa completa y suficiente en el Reporte de operaciones sospechosas") en www.fincen.gov.

PROHIBISIÓN DE REVELAR LOS INFORMES ROS

Ningún banco o director, funcionario, empleado o agente del mismo que reporte una transacción sospechosa está autorizado para informar a la(s) persona(s) involucradas en dicha transacción que la transacción ha sido reportada. Por lo tanto, toda persona a quien se dirija una orden judicial solicitándole divulgar un informe ROS o la información que contiene uno de estos informes, o que de otra forma esté emplazada para hacerlo, salvo cuando dicha revelación sea solicitada por FinCEN o una autoridad apropiada o agencia bancaria federal, deberá rehusarse a entregar dicho informe ROS o a suministrar información alguna que pueda revelar que se ha elaborado o radicado un informe ROS, y para ello citará 31 CFR 103.18(e) y 21 USC 5318(g)(2). Se debe informar a FinCEN así como a la agencia bancaria federal del banco respectivo sobre la existencia de dicha solicitud, así como sobre la respuesta dada por el banco. Además, FinCEN y las agencias bancarias federales consideran que los controles internos del banco relativos a la radicación de los informes ROS deben minimizar los riesgos de la divulgación respectiva.

RETENCIÓN DE REGISTROS Visión general fundamental – Informes de transacciones en moneda

OBJETIVO

Evaluar el cumplimiento del banco con los requisitos estatutarios y regulatorios fijados para los informes sobre grandes volúmenes de transacciones en moneda.

VISIÓN GENERAL

Todo banco debe elaborar un Informe de Transacciones en Moneda (CTR en inglés por Currency Transaction Report) (Formulario 104 de FinCEN) por cada transacción en

moneda[53] (depósito, retiro, intercambio u otros pagos o transferencias) de más de US $ 10.000 efectuada por el banco o a través del mismo o dirigida al mismo. No es necesario reportar algunas transacciones, como las que incluyen a "personas exentas", agrupación que puede incluir a clientes minoristas o comerciales que cumplen con ciertos criterios específicos fijados para la exención. Ver la sección de visión general fundamental titulada "Exención del Informe de transacciones en moneda" en la página
51.

AGREGACIÓN DE TRANSACCIONES EN MONEDA

Cuando en un mismo día hábil ocurren múltiples transacciones en moneda por un valor superior a los US $ 10.000 éstas se deben tratar como si fueran una sola transacción, si el banco sabe que han sido realizadas por una misma persona o en nombre de ésta. Para determinar transacciones múltiples es necesario agregar las transacciones realizadas a través de todo el banco. Los tipos de transacciones en moneda que están sujetos a los requisitos del informe, tanto individual como agregado, incluyen los siguientes, sin limitarse únicamente a ellos: cuentas individuales de retiro (IRA en inglés), pagos de préstamos, transacciones efectuadas en cajeros automáticos (ATM en inglés), compras de certificados de depósito, depósitos y retiros, transferencias de fondos pagadas en moneda y compras de instrumentos monetarios. Se considera altamente recomendable que los bancos desarrollen sistemas que les permitan agregar transacciones en moneda realizadas por toda la entidad. La gerencia debe asegurarse de que exista un sistema que permita reportar adecuadamente las transacciones de moneda que están sujetas a los requisitos fijados por la Ley del Secreto Bancario.

REQUISITOS DE PLAZO DE RADICACIÓN Y RETENCIÓN DE REGISTROS

El Informe de transacciones en moneda (CTR) debe radicarse ante FinCEN durante los quince (15) días siguientes a la fecha de la transacción (o para los veinticinco (25) días de la misma, si se radica en forma magnética o electrónica). El banco debe guardar copias de los CTR durante cinco (5) años a partir de la fecha del informe (31 CFR 103.27 (a)(3)).

[53] Moneda significa el dinero representando en monedas y billetes de los Estados Unidos o de cualquier otro país, siempre y cuando sea aceptado normalmente como moneda en el país que lo emitió.

Si un banco no ha radicado informes CTR sobre transacciones reportables, debe iniciar la radicación de los mismos y comunicarse con el Centro de Cómputo de Detroit[54] del fisco de EE. UU. [Servicio de Ingresos Nacionales -IRS en inglés] para solicitar una determinación en cuanto a la posible necesidad de radicar transacciones previas no reportadas.

[54] El Centro de Cómputo de Detroit del Servicio de Ingresos Nacionales (IRS en inglés) es el lugar en donde reposan todos los informes sobre la Ley el Secreto Bancario que todo banco está obligado a radicar. Para comunicarse con el Centro de Cómputo de Detroit se puede llamar al teléfono 800-800-28
77.

Visión general fundamental – Exención del Informe de transacciones en moneda

OBJETIVO

Evaluar el cumplimiento del banco con los requisitos estatutarios y regulatorios fijados para la exención de los requisitos del Informe de transacciones en moneda.

VISIÓN GENERAL

Históricamente, las normas del Departamento del Tesoro de los Estados Unidos han reconocido el hecho de que la elaboración rutinaria de informes sobre transacciones de gran volumen no necesariamente ayuda a las autoridades y puede generar cargas poco razonables para los bancos. Por consiguiente, es posible que los bancos eximan a ciertos tipos de clientes de la necesidad de reportar las transacciones efectuadas en moneda.

La Ley sobre la Eliminación del Lavado de Dinero de 1994 (MLSA en inglés) creó un proceso de exención de dos (2) fases. Las exenciones de la Fase I eximen a las transacciones en moneda realizadas por bancos, oficinas y agencias gubernamentales y empresas públicas o empresas que cotizan en la bolsa, así como las subsidiarias de las mismas. Bajo las exenciones de la Fase II quedan exentas las transacciones en moneda realizadas por empresas más pequeñas que cumplen con ciertos criterios fijados por las normas de FinCEN. Para poder eximir a un cliente del requisito de elaboración y radicación de informes CTR [Informes de transacciones en moneda], los bancos deben radicar el formulario de Designación de persona exenta [Designation of Exempt Person] (TD F 90-22.53).

EXENCIONES DEL CRT DE LA FASE I (31 CFR 103.22 (d)(2)(i)-(v))

Las normas de FinCEN identifican cinco categorías de entidades exentas en la Fase I:

. • Los bancos, hasta donde sea pertinente según el alcance de sus operaciones nacionales.
. • Las entidades o departamentos oficiales de nivel federal, estatal o local.
. • Cualquier entidad que ejerza autoridad gubernamental en los Estados Unidos.
. • Cualquier entidad (que no sea entidad bancaria) cuyas acciones comunes se coticen en las bolsas de Nueva York, American Stock Exchange o Nasdaq (con algunas excepciones).
. • Cualquier subsidiaria (diferente a un banco) de cualquier "entidad que cotice en la bolsa" y se rija bajo las leyes de Estados Unidos, cuyas acciones comunes sean como

mínimo un 51% de propiedad de la entidad que cotiza.

Plazos para radicar informes

Los bancos deben radicar un formulario de Designación de entidad exenta para eximir a una entidad de Fase I de la obligación de radicar el Informe de transacciones de moneda. La exención de la entidad de Fase I cubre todas las transacciones realizadas en moneda con la entidad exenta, y no sólo las transacciones en moneda realizadas a través de una cuenta. El formulario se debe radicar ante el organismo tributario de EE. UU. [Servicio de Ingresos Nacionales -IRS por su sigla en inglés] durante los treinta (30) días siguientes a la realización de la primera transacción en moneda de la cual el banco desea quedar exento.

Revisión anual

Al menos una vez al año el banco debe revisar y verificar la información que sustenta las designaciones de las personas o entidades exentas de la Fase I.

EXENCIONES CTR DE LA FASE II (31 CFR 103.22(d)(2)(vi)-(vii))

Los negocios que no caben en ninguna de las categorías de la Fase I de todas formas pueden quedar cobijados por las exenciones de la Fase II si califican como "negocios que no cotizan en la bolsa" o como "clientes de nómina".

Negocios que no cotizan en la bolsa

Los "negocios que no cotizan en la bolsa" se definen como empresas comerciales, según el alcance de sus operaciones nacionales y únicamente con respecto a las transacciones realizadas a través de sus cuentas exentas, que (i) han mantenido una cuenta de transacción en el banco de la exención durante al menos doce (12) meses, (ii) con frecuencia[55] efectúan transacciones en moneda con el banco por un valor superior a US $ 10.000 y (iii) han sido constituidas bajo las leyes de los Estados Unidos o de algún estado de los Estados Unidos, o están registradas en los Estados Unidos o en algún estado de ese país y son elegibles para realizar negocios en ese país o un estado del mismo.

Negocios que no califican

Ciertos negocios no califican para la exención otorgada a los negocios que no cotizan en la bolsa (31 CFR 103.22(d)(6)(viii)). Dichos negocios no elegibles se definen como negocios dedicados principalmente a una o más de las siguientes actividades concretas:

. • servir como entidades financieras o agentes de entidades financieras de cualquier tipo;

. • compraventa de vehículos automotores de cualquier tipo, así como de embarcaciones, aviones, maquinaria agrícola o casas móviles;
. • ejercer el derecho, la contabilidad o la medicina;
. • subastar bienes;
. • alquilar u operar embarcaciones, buses o aviones como charters; • operar servicios de intermediación de casas de empeño;

[55] FinCEN expidió una directiva ("Guía para interpretar [el término] 'frecuentemente' en los criterios para la exención de los 'Negocios que no cotizan en la Bolsa' bajo 31 CFR 103.22 (d)(2)(vi)(B), noviembre de 2002", www.fincen.gov), en la cual se expresa lo siguiente: "En general, los clientes que están sujetos a la exención como negocios que no cotizan en la Bolsa deben realizar al menos ocho (8) transacciones voluminosas en moneda durante el año. Esto básicamente significa que dichos clientes deben llevar a cabo una transacción voluminosa en moneda aproximadamente cada seis (6) semanas. El hecho de que un cliente realice menos de ocho grandes transacciones en moneda al año generalmente revela que dichas transacciones voluminosas en moneda no responden a una necesidad recurrente o rutinaria".

. • dedicarse a cualquier clase de juegos (distintos a las apuestas "pari-mutuel" licenciadas realizadas en pistas de carreras);
• participar en servicios de asesoría sobre inversiones o servicios de banca de inversión; • operar servicios de intermediación de finca raíz; • operar en actividades de títulos de seguros y cierres de finca raíz;
. • participar en actividades realizadas por sindicatos;
. • participar en cualquier otra actividad que pueda ocasionalmente indicar FinCEN.

Las entidades que realicen múltiples actividades de negocios pueden calificar para la exención como negocios que no cotizan la bolsa, siempre y cuando más del 50% de sus ingresos brutos anuales[56] se deriven de una o más de las actividades comerciales no elegibles listadas bajo la regla.

Clientes de nómina

Los "clientes de nómina" se definen únicamente con base en retiros realizados para fines de nómina desde cuentas actuales cubiertas por la exención. Se trata de entidades que: (i) han mantenido una cuenta de transacciones en el banco durante por lo menos doce (12) meses; (ii) operan empresas que regularmente retiran más de US $ 10.000 para pagar a sus empleados de Estados Unidos en esa moneda; y (iii) han sido constituidas bajo las leyes de los Estados Unidos o de algún estado de ese país o están registradas en Estados Unidos o en algún estado de ese país y son elegibles para realizar negocios en ese país o un estado del mismo.

Plazo para radicar informes

Luego de decidir eximir a un cliente de Fase II, el banco debe radicar un formulario de Designación de entidad exenta (TD F 90-22.53) durante los treinta (30) días siguientes a la realización de la primera transacción de cliente que el banco desee eximir.

Revisión anual

Al menos una vez al año el banco deberá revisar y verificar la información que sustenta cada designación de entidad exenta de la Fase II. Sin embargo, para ser consistente con esta revisión anual, el banco debe revisar y constatar al menos una vez al año que la gerencia efectivamente le hace seguimiento a las cuentas de Fase II en cuanto a transacciones sospechosas.

Revisiones cada dos años

[56] Con frecuencia surgen interrogantes sobre lo que significan los "ingresos brutos" de las actividades de juego, tales como las ventas de lotería. FinCEN ha establecido que para los fines de determinar si un negocio deriva más del 50% de sus ingresos brutos de actividades de juego, el término ingresos brutos incluye el monto de dinero realmente obtenido como ingresos por una entidad a partir de una actividad particular, en lugar del volumen de ventas de dichas actividades que realice el negocio. Por ejemplo, si un negocio participa en ventas de lotería, los "ingresos brutos" derivados de esta actividad serían el monto de dinero que ese negocio realmente obtiene de las ventas de lotería, en lugar del monto de dinero que obtiene en nombre del sistema de lotería del Estado o destinado al mismo. Ver Regla FinCEN 2002-1, www.fincen.gov.

Además, para los clientes de Fase II es necesario radicar nuevamente el formulario cada dos (2) años, a más tardar el 15 de marzo, como parte del proceso de revisión bianual. Bajo el proceso de revisión bianual que aplica para los clientes de Fase II, el banco debe incluir la siguiente información en dicha renovación bianual: (i) todo cambio relativo al control de la entidad exenta que sea del conocimiento del banco (o sobre el cual el banco tiene razones para conocer esa información) y (ii) una certificación por medio de la cual se hace constar que el banco efectivamente ha aplicado su sistema de monitoreo de actividades sospechosas a las transacciones en moneda de la entidad exenta, según haya sido necesario hacerlo, pero como mínimo, una vez al año.

PUERTO SEGURO POR NO RADICACIÓN DE LOS CTR

Las reglas (31 CFR 103.22(d)(8)) ofrecen protección o “puerto seguro” [safe harbor] en el sentido de que los bancos no son responsables por no radicar CTR sobre transacciones en moneda realizadas por entidades exentas, salvo si el banco conscientemente suministra información falsa o incompleta o considera posible que el cliente no cumpla con las condiciones que se requieren para ser cliente exento. Si no existe información específica que indique que el cliente ya no cumple con los requisitos de entidad exenta, el banco tiene derecho a un “puerto seguro” [quedar exento de responsabilidad] con respecto a cualquier sanción civil que aplique para la exención si continúa tratando al cliente como cliente exento hasta la fecha de la revisión anual del cliente.

EFECTOS SOBRE OTROS REQUISITOS REGULATORIOS

Los procedimientos de exención no crean exenciones ni producen efecto alguno sobre la obligación de los bancos de radicar sus Reportes de operaciones sospechosas (ROS). Por ejemplo, el hecho de que un cliente sea entidad exenta no produce efecto alguno sobre la obligación que pesa sobre el banco de mantener registros de las transferencias de fondos efectuadas por dicha entidad, ni sobre la obligación de retener los registros relacionados con la venta de instrumentos monetarios a dicha entidad.

Si un banco incorrectamente exime una cuenta, es posible que el examinador solicite a la gerencia revocar la exención. En todo caso el banco debe iniciar la radicación de sus informes CTR y ponerse en contacto con el Centro de Cómputo de Detroit[57] del Servicio de Ingresos Nacionales (el fisco de EE. UU. cuya sigla es IRS en inglés) para solicitar una determinación en cuanto a la necesidad de radicar las transacciones no reportadas con retroactividad.

En la página web del FinCEN en la dirección www.FinCEN.gov es posible encontrar información adicional sobre el proceso de exención de las transacciones en moneda.

[57] El Centro de Cómputo de Detroit del Servicio de Ingresos Nacionales de EE. UU. (IRS por sus siglas en inglés) es un repositorio central de informes BSA (sobre la Ley del Secreto Bancario) que deben radicar los bancos. Para comunicarse con el Centro de Cómputo de Detroit favor llamar al 800-800-2877.

Visión general fundamental – Información compartida

OBJETIVO

Evaluar el cumplimiento de la entidad financiera con los requisitos estatutarios y regulatorios fijados para los "Procedimientos especiales para compartir información con el fin de disuadir el Lavado de dinero y las actividades terroristas" (sección 314 sobre Solicitudes de información).

VISIÓN GENERAL

El 26 de septiembre de 2002 entró en vigencia el reglamento definitivo destinado a implementar la sección 314 de la Ley Patriota (31 CRF 103.100 y 31 CRF 103.110). Dicho reglamento fijó los procedimientos a emplear para compartir información con el fin de disuadir el lavado de dinero y las actividades terroristas.

INFORMACIÓN COMPARTIDA ENTRE AUTORIDADES POLICIALES Y ENTIDADES FINANCIERAS – SECCIÓN 314(a) DE LA LEY PATRIOTA (31 CFR

103.100)

Las autoridades policiales federales que investigan actividades terroristas o lavado de dinero pueden solicitarle a FinCEN que, en su nombre, solicite información específica a entidades financieras o agrupaciones de dichas entidades. Las autoridades policiales deben entregar una certificación a FinCEN declarando que existe evidencia creíble de participación en actividades terroristas o lavado de dinero, o la sospecha razonable de lo mismo, por cada individuo, entidad u organización sobre la cual procuran obtener información. También deben suministrar identificadores concretos, tales como fechas de nacimiento y direcciones, para permitirle a la entidad financiera diferenciar entre nombres compartidos o similares. Al recibir certificados debidamente elaborados de parte de las autoridades policiales, FinCEN puede proceder a solicitarle a las entidades financieras que examinen sus registros para ver si en ellas tienen cuentas o han participado en transacciones alguna(s) persona(s), entidad(es) u organización(ciones) especificada(s).

Al recibir una solicitud de información, las entidades financieras deben realizar una sola búsqueda en ese momento en sus registros para identificar cuentas o transacciones relativas a un sospechoso que haya sido nombrado. Salvo si se expiden instrucciones distintas en la solicitud de información, las entidades financieras deben examinar sus registros en busca de cuentas corrientes y otras cuentas mantenidas durante los doce
(12) meses anteriores, así como transacciones realizadas por fuera de las cuentas, por parte de la persona o entidad sospechosa nombrada o en nombre de la misma, durante los seis (6) meses anteriores. Las entidades financieras tienen un plazo de catorce (14) días para buscar en sus registros y reportar a FinCEN cualquier acierto que se encuentre, salvo si la solicitud de información indica otra cosa.

FinCEN le ha entregado a las entidades financieras un documento de Instrucciones generales y Preguntas frecuentes (FAQ) relativas al proceso de la sección 314(a). Salvo si las instrucciones de la solicitud de información solicitan otra cosa, las entidades financieras deben buscar los registros que se especifican en dichas Instrucciones generales. Las entidades financieras pueden obtener copias adicionales o de reemplazo de las Instrucciones generales o las FAQ a través de FinCEN.

Si una entidad financiera identifica alguna cuenta o transacción, debe informarle a FinCEN que tiene un resultado positivo. No es necesario daar a FinCEN ningún otro detalle al respecto. Basta con informar que la entidad financiera tiene un acierto. Si los resultados son negativos no es necesario enviar respuesta. Las entidades financieras pueden suministrar una lista de sospechosos nombrados a un tercero proveedor o distribuidor de servicios para que éste se encargue de realizar la búsqueda de los registros, siempre y cuando la entidad financiera adopte las medidas necesarias, mediante un contrato u otros procedimientos, para asegurar que dicho tercero salvaguarde y mantenga la confidencialidad de la información respectiva.

Las entidades financieras deben desarrollar e implementar políticas, procedimientos y procesos integrales en respuesta a las solicitudes formuladas con base en la sección 314(a). La regulación restringe los posibles usos de la información suministrada bajo una solicitud

de la sección 314(a) (31 CFR 103.100(b)(2)(iv))[58]. El único uso que las entidades financieras podrán darle a la información es para reportar la información solicitada a FinCEN, para determinar si se puede proceder a establecer o mantener una cuenta o participar en una transacción, o para colaborar con el cumplimiento de la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero (BSA/AML). Si bien es posible utilizar la lista de la sección 314(a) para determinar si se debe establecer o mantener una cuenta, FinCEN se opone enfáticamente al empleo de dicha lista por parte de las entidades financieras como único factor conducente a una decisión al respecto, a menos que la solicitud específicamente indique lo contrario. A diferencia de las listas de la OFAC, las listas de la sección 314(a) no son "listas de alerta" permanentes. De hecho, las listas de la sección 314(a) generalmente tienen que ver con consultas que se realizan en una sola ocasión, y no se actualizan ni se corrigen cuando se suspende una investigación, se rechaza un proceso judicial o se exonera a una persona o entidad. Además, los nombres que aparecen en dichas listas no representan a personas o entidades que han sido formalmente acusadas o encontradas culpables; más bien, sobre las personas o entidades que aparecen en las listas 314(a) apenas pesa una "sospecha razonable" basada en evidencia creíble que apunta hacia participación en actos terroristas o lavado de dinero. Además, FinCEN advierte que el hecho de ser incluido en una lista de la sección 314(a) no debe convertirse en el único factor utilizado para determinar si es necesario radicar un Reporte de Operaciones Sospechosas (ROS). Las entidades financieras deben establecer procesos para determinar si es necesario radicar el Reporte de operaciones sospechosas y cuándo hacerlo.

Las acciones realizadas de conformidad con la información que contienen las solicitudes provenientes de FinCEN no afectan las obligaciones que tienen las entidades financieras de cumplir con todas las demás reglas y el reglamento de la OFAC, ni afectan tampoco las obligaciones que tienen las entidades financieras de responder ante cualquier proceso jurídico que se pueda presentar. Además las acciones adoptadas como respuesta a las solicitudes recibidas no exoneran a las entidades financieras de su

[58] Cuando en las solicitudes se mencionan múltiples sospechosos, con frecuencia se las denomina "listas 314(a)".
Las entidades financieras no podrán revelar a ninguna persona o entidad distinta a FinCEN, al regulador bancario primario de la entidad o a la autoridad o agencia Federal en cuyo nombre FinCEN solicita la información, el hecho de que FinCEN ha solicitado
o ha obtenido dicha información. Las entidades financieras deben designar a uno o más contactos para recibir las solicitudes de información. FinCEN ha informado que un grupo de entidades financieras afiliadas puede establecer un solo punto de contacto para distribuir las listas de la sección 314(a) y proceder a responderlas. Sin embargo, las listas de la sección 314 (a) no se pueden compartir con ninguna oficina, sucursal o afiliada en el extranjero (salvo si la solicitud específicamente establece otra cosa), y tampoco pueden compartirse con entidades afiliadas o subsidiarias de empresas *holding* de bancos, si dichas afiliadas o subsidiarias no son entidades financieras según lo descrito en 31 USC 5312(a)(2).

Cada entidad financiera debe contar con procedimientos apropiados para proteger la seguridad y confidencialidad de las solicitudes que reciba de FinCEN. Los procedimientos

dirigidos a asegurar la confidencialidad se considerarán apropiados si la entidad financiera aplica procedimientos similares a los que ha establecido para cumplir con la sección 501 de la Ley Gramm-Leach-Bliley (15 USC 6801) sobre la protección de la información personal no pública de sus clientes. Las entidades financieras pueden llevar un registro de todas las solicitudes de información de la sección 314(a) que reciban, así como de los resultados positivos o aciertos que hayan presentado y reportado a FinCEN.

Además, es esencial contar con documentación que pueda demostrar que todas las búsquedas requeridas se han realizado. Esto se puede lograr guardando copias de la página de presentación de la solicitud, conjuntamente con una página en blanco usada a manera de verificación, en la cual se indica mediante una firma que los registros fueron verificados, la fecha de la búsqueda y los resultados de la misma (por ejemplo, positivos
o negativos). Para los aciertos, es necesario guardar copia del formulario que se devuelve a FinCEN, así como de la documentación de soporte. Si la entidad financiera opta por guardar copias de las solicitudes de la sección 314(a), no se la debe criticar por hacerlo, siempre y cuando las proteja adecuadamente con medidas de seguridad para salvaguardar su confidencialidad. Las auditorías deben incluir una evaluación del cumplimiento de estas pautas, dentro del alcance de las mismas.

En marzo del 2005, FinCEN empezó a distribuir listas de la sección 314(a) a través de un sitio web seguro. Cada dos semanas o si se transmite una solicitud urgente, el contacto designado por el banco recibirá una notificación de FinCEN indicando que hay anuncios nuevos sobre al tema en el sitio seguro de Internet de FinCEN. El contacto podrá conocer las listas de la sección 314 (a) previa y actual y descargar los archivos en distintos formatos para realizar las búsquedas. Además, los bancos pueden utilizar el sitio web de FinCEN para notificar a FinCEN sobre resultados positivos. Los bancos que reciben las listas de temas de la sección 314 (a) por fax seguirán recibiéndolas por este medio.

INFORMACIÓN COMPARTIDA VOLUNTARIAMENTE -SECCIÓN 314 (de) DE LA LEY PATRIOTA (31 CFR 103.110)

La sección 314 (b) estimula a las entidades financieras y asociaciones de entidades financieras ubicadas en los Estados Unidos a compartir información que permita identificar y reportar operaciones que puedan estar relacionadas con actividades terroristas o lavado de dinero. La sección 314(b) también ofrece protección específica en cuanto a responsabilidad civil. Para beneficiarse de este "puerto seguro" estatutario que protege contra esta responsabilidad, las entidades financieras o asociaciones respectivas deben notificar a FinCEN sobre su intención de compartir información, agregando que han establecido y mantendrán procedimientos adecuados para proteger la seguridad y confidencialidad de la información. El incumplimiento de los requerimientos de 31 CFR 103.110 implica la pérdida del "puerto seguro" que protege contra las consecuencias que puede acarrear el hecho de compartir información, lo que puede redundar en una violación de las leyes de la privacidad y otras leyes y regulaciones.

Si una entidad financiera opta por participar voluntariamente en la sección 314(b), dicha entidad debe desarrollar e implementar políticas, procedimientos y procesos para compartir y recibir información.

La notificación de la intención de compartir información tiene una validez de un (1) año[60]. La entidad financiera debe designar un contacto para recibir y suministrar información. Es necesario que las entidades financieras fijen procesos para el envío y recibo de solicitudes para compartir información. Además, deben adoptar medidas razonables para verificar que las entidades o asociaciones con las cuales se proponen compartir información a su vez entreguen la notificación respectiva a FinCEN. A las entidades financieras que participan en este proceso, FinCEN les permite acceder a un listado de las demás entidades financieras participantes y la información de contacto respectiva de las mismas.

Si una entidad financiera recibe esta información proveniente de otra, la que recibe la información está obligada a limitar el uso dado a dicha información y mantener la seguridad y confidencialidad de la misma (ver 31 CFR 103.110(b)(4)). La información puede utilizarse únicamente para identificar, y donde sea apropiado, reportar sobre el lavado de dinero y actividades terroristas; para determinar si establecer o mantener una cuenta; para realizar una transacción; o para asistir con el cumplimiento de la Ley del Secreto Bancario. Los procedimientos dirigidos a asegurar la confidencialidad se considerarán apropiados si la entidad financiera aplica procedimientos similares a los que ha establecido para cumplir con la sección 501 de la Ley Gramm-Leach-Bliley (15 USC 6801) relativa a la protección de la información personal no pública de sus

[59] Favor referirse al sitio de Internet de FinCEN en www.fincen.gov para obtener información sobre los puntos de contacto sobre la sección 314(a) de cada regulador primario.

[60] Las instrucciones para la entrega del formulario de notificación se pueden ver en el sitio de Internet de FinCEN en www.fincen.gov.

clientes. El "puerto seguro" no cubre la información que se comparte con otros países. Además, la sección 314(b) no autoriza a las entidades financieras a compartir los ROS ni revelar la existencia o no existencia de los mismos. Si las entidades financieras comparten información bajo la sección 314(b) sobre un ROS elaborado o radicado, la información que se comparte deberá limitarse a datos subyacentes sobre transacciones o clientes. Las entidades financieras pueden utilizar la información lograda bajo la sección 314(b) para decidir si radicar un ROS o no, pero la intención de elaborar o radicar un ROS no se puede compartir con otras entidades financieras. Es necesario que las entidades financieras fijen procesos para determinar si deben radicar un ROS y cuando hacerlo.

Las acciones realizadas con respecto a la información obtenida a través del proceso de compartir información voluntariamente no afectan la obligación que tienen las entidades financieras de responder ante un proceso jurídico. Además, las acciones adoptadas en respuesta a la información obtenida a través del proceso de compartir información voluntariamente no eximen a las entidades financieras de su obligación de radicar los ROS e inmediatamente informar a las autoridades, de ser necesario, de conformidad con todas las leyes y reglamentos aplicables.

Visión general fundamental – Compraventa de instrumentos monetarios

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios de registro de información necesarios para la compraventa de instrumentos monetarios de moneda en montos de US $3.000 a $10.000, inclusive. Esta parte cubre los requisitos regulatorios establecidos en la Ley del Secreto Bancario. Favor referirse a la sección ampliada de este manual para ver discusiones y procedimientos adicionales sobre ciertos riesgos relativos al lavado de dinero inherentes a las actividades de compra y venta de instrumentos monetarios.

VISIÓN GENERAL

Los bancos venden una variedad de instrumentos financieros (por ejemplo, cheques, incluyendo cheques en moneda extranjera, giros postales, cheques de gerencia y cheques viajeros) a cambio de moneda. La compra de estos instrumentos por montos inferiores a los US $10.000 es una práctica común empleada por quienes lavan dinero, para evadir los requisitos de reporte que aplican para las transacciones de grandes volúmenes. Una vez se obtienen los instrumentos, los delincuentes típicamente los depositan en cuentas abiertas en otros bancos para facilitar el movimiento de los fondos a través del sistema de pagos. En muchos casos las personas involucradas no poseen cuentas en el banco que les vende los instrumentos.

IDENTIFICACIÓN DEL COMPRADOR

Bajo 31 CFR 103.29 los bancos están obligados a verificar la identidad de quienes compran instrumentos monetarios a cambio de efectivo por valores entre US $3.000 y US $ 10.000 inclusive, y llevar registros de dichas ventas.

Los bancos pueden verificar si el comprador de los instrumentos monetarios posee cuenta de depósito con su respectiva identificación de cuenta habiente registrada en el banco, o pueden identificar la identidad del comprador viendo el documento de identidad del mismo, el cual debe incluir el nombre y la dirección del cliente, según el documento que sea reconocido por la comunidad financiera como medio de identificación válido para el pago de cheques a quienes no son clientes. El banco debe obtener información adicional de los compradores que no poseen cuentas de depósito. El método empleado para verificar la identidad del comprador debe quedar registrado.

IDENTIFICACIÓN ACEPTADA

El Dictamen administrativo [Administrative Ruling] 92-1 expedido por la Tesorería de los Estados Unidos indica la forma en que los bancos pueden verificar la identidad de clientes de tercera edad o discapacitados que no posean documentos de identidad aceptables. Los bancos pueden aceptar la tarjeta del Seguro Social o de Medicare/Medicaid conjuntamente con alguna otra forma de identificación que incluya el nombre y la dirección del cliente. Esa identificación adicional puede consistir en recibos de pago de servicios públicos,

recibos de pago de impuestos o la tarjeta de registro para votar en elecciones. Las formas alternas de identificación que decida aceptar un banco deben quedar incluidas en sus políticas, procedimientos y procesos formales.

COMPRAS SIMULTÁNEAS

Las compras simultáneas de un mismo instrumento o instrumentos de distintas clases por un valor total de US $ 3.000 o más deben tratarse como una sola compra. Las compras múltiples realizadas en un mismo día hábil por valor de US $ 3.000 o más deben agregarse y tratarse como una sola compra, si el banco tiene conocimiento de las mismas.

COMPRAS INDIRECTAS DE INSTRUMENTOS MONETARIOS EN MONEDA

Los bancos pueden implementar una política que exija a los clientes con cuentas de depósito que desean adquirir instrumentos monetarios por un valor entre US $ 3.000 y US $ 10.000, que primero depositen el monto respectivo en sus propias cuentas de depósito. No hay nada en la Ley del Secreto Bancario ni en la reglamentación de la misma que prohíba a los bancos instituir una política de este tipo.

Sin embargo, FinCEN considera[61] que cuando un cliente compra un instrumento monetario por un monto entre US $ 3000 y US $ 10.000 con fondos que ya ha depositado en su propia cuenta, de todas formas la transacción está sujeta a los requisitos de registro establecidos en 31 CFR 103.29. Estos requisitos aplican tanto si la transacción se realiza de conformidad con las políticas establecidas por el banco, como si se realiza por solicitud del cliente. En términos generales, cuando los bancos le venden instrumentos monetarios a clientes que poseen cuentas de depósito, los mismos bancos ya tienen la mayor parte de la información que se requiere según 31 CFR 103.29, lograda durante el curso normal de sus negocios.

REQUISITOS DE REGISTROS Y RETENCIÓN DE LA INFORMACIÓN

Según 31 CFR 103.29 los registros de ventas de los bancos deben incluir, como mínimo, la siguiente información:

• Si el comprador **posee una cuenta de depósito** en el banco:

- Nombre del comprador
- Fecha de la compra
- Tipo de instrumento adquirido
- Número de serie de cada uno de los instrumentos adquiridos
- Monto en dólares de cada instrumento adquirido en moneda
- Información específica de identificación, si aplica.[62]

La "Guía para la interpretación de las políticas de las entidades financieras sobre los requisitos de retención de información bajo 31 CFR 103.29" de noviembre de 2002 de FinCEN, www.fincen.gov.

[62] El banco debe verificar que la persona tenga una cuenta de depósito o verificar la identidad de dicha persona. La verificación puede hacerse mediante una tarjeta de firma u otro tipo de archivo o registro del

• Si el comprador **no posee cuenta de depósito** en el banco:

– Nombre y dirección del comprador – número de Seguro Social o cédula de extranjería del comprador – Fecha de nacimiento del comprador – Fecha de la compra – Tipo de instrumento adquirido – Número de serie de cada uno de los instrumentos adquiridos – Monto en dólares de cada instrumento adquirido en moneda – Información específica de identificación para verificar la identidad del comprador (por ejemplo, estado que expide la licencia de conducción y número de la misma).

Si el comprador no produce la información requerida en el momento de la transacción o ésta no se obtiene de los registros previamente verificados del mismo banco, se debe rechazar la transacción. Los registros de ventas de instrumentos monetarios deben guardarse durante cinco (5) años y estar disponibles para consulta por parte de las entidades apropiadas mediante solicitud.

banco, siempre que el nombre y la dirección del cliente que posee cuentas de depósito hayan sido verificados previamente y la información haya sido registrada en la tarjeta de firma u otro archivo o registro, o mediante examen del documento normalmente aceptado en la comunidad bancaria que contenga el nombre y la dirección del comprador. Si la identidad del cliente que tiene cuenta de depósito no ha sido verificada con anterioridad, el banco debe registrar la información concreta de identificación (por ejemplo, el estado que

expidió la licencia de conducción así como el número de la misma) del documento examinado.

Visión general fundamental – Transferencias de fondos

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios establecidos para las transferencias de fondos. Esta sección cubre los requisitos regulatorios establecidos por la Ley del Secreto Bancario. Favor referirse a las secciones ampliadas de este manual para conocer discusiones y procedimientos relativos a los riesgos específicos de lavado de dinero que son inherentes a las actividades de transferencias de fondos.

VISIÓN GENERAL

Los sistemas de transferencias de fondos permiten transferencia instantánea de fondos, tanto nacionales como internacionales. Por lo tanto estos sistemas pueden convertirse en métodos atractivos para ocultar el origen de fondos derivados de actividades ilícitas. La Ley del Secreto Bancario fue enmendada por la Ley Annunzio-Wylie Contra el Lavado de Dinero de 1992, con el objetivo de facultar a la Tesorería de los Estados Unidos y a la Junta de la Reserva Federal para regular las transferencias de fondos tanto nacionales como internacionales.

En 1995 la Tesorería de los Estados Unidos y la Junta de Gobernadores del Sistema de la Reserva Federal expidieron una reglamentación definitiva sobre requisitos de registros para órdenes de pago emitidas por bancos (31 103 33).[63] La reglamentación requiere que cada banco que participe en transferencias de fondos[64] recaude y retenga cierta información sobre las transferencias de fondos realizadas por valor de US $ 3.000
o más.[65] La información que es necesario obtener y retener depende del papel que ejerza el banco en la transferencia de fondos concreta (banco originador, banco intermediario o

[63] 31 CRF 103.33(e) es la regla que rige los registros que llevan los bancos, y 31 CFR 103.33(f) impone requisitos similares a las entidades financieras no bancarias que participan en transferencias de fondos. Los procedimientos establecidos en la visión general fundamental únicamente tratan las reglas que aplican para los bancos bajo 31 CFR 103.33(e).

[64] La transferencia de fondos se define en 31 CRF 103.11. Las transferencias de fondos que se rigen por la Ley de Transferencia Electrónica de Fondos de 1978, así como todas las demás transferencias de fondos realizadas a través de cámaras de compensación automáticas, cajeros automáticos o sistemas de puntos de venta, están excluidas de esta definición y quedan exentas de los requisitos establecidos en 103.33(e), (f) y (g).

31 CRF 103.33(e)(6) crea excepciones a los requerimientos para las transferencias de fondos. Las transferencias de fondos en las que el originador y el beneficiario son la misma persona y el banco del primero y del segundo son el mismo banco, no están sujetas a los requisitos de registros que aplican para las transferencias de fondos. Además, se crean excepciones a los requisitos de registro de transferencias de fondos cuando tanto el originador como el beneficiario son: bancos; una subsidiaria nacional de entera

propiedad de un banco constituido en los Estados Unidos; agente o comisionista de valores; subsidiaria nacional de entera propiedad de un agente o comisionista de valores; los Estados Unidos; un gobierno estatal o local; o una agencia o instrumentalidad oficial de nivel federal, estatal o local.

También en 1995 la Tesorería de los Estados Unidos expidió una regla definitiva en la que exigió a todas las entidades financieras incluir cierta información en las órdenes de transmisión de transferencias de fondos efectuadas por valor de US $ 3.000 o más (31 CFR 103.33).67 Este requisito es conocido en general como la "Regla para viajes" [“Travel Rule”].

OBLIGACIONES DE LOS BANCOS ORIGINADORES

Requerimientos en cuanto a registros

Por cada orden de pago por valor de US $3.000 o más que un banco acepte realizar como banco originador, dicho banco debe obtener y guardar los siguientes registros (31 CFR 103.33(e)(1)(i)):

- Nombre y dirección del originador
- Monto de la orden de pago
- Fecha de la orden de pago
- Instrucciones de pago
- Identidad de la entidad beneficiaria
- Los siguientes elementos, en la cantidad que se reciba con la orden de pago:

  – Nombre y dirección del beneficiario
  – Número de cuenta del beneficiario
  – Cualquier otra identificación específica del beneficiario

Registros adicionales para clientes no establecidos

Si el originador no es un cliente establecido del banco, es necesario obtener y retener la información mencionada arriba. Además, el banco del originador debe recaudar y retener otra información adicional, dependiendo de si la orden de pago se hace personalmente.

<u>Órdenes de pago realizadas personalmente</u>

Si la orden de pago se hace personalmente, el banco del originador debe verificar la identidad de quien coloca la orden para poderla aceptar. Si acepta la orden, la entidad financiera del originador debe obtener y retener los siguientes registros:

- Nombre y dirección de quien coloca la orden
- Tipo de identificación revisada

[66] Estos términos están definidos bajo 31 CFR 103.11. [67] La regla aplica tanto para bancos como para entidades no bancarias (31 CFR 103.33(g)). Debido a su mayor alcance, la Regla para Viajes emplea términos de mayor

cobertura tales como "orden de transmisión" [“transmittal order”] en lugar de "orden de pago" y “entidad financiera del transmisor” [“transmittor’s financial institution”] en lugar de “banco originador”. Los términos más amplios incluyen los de naturaleza específicamente bancaria.

. • Número del documento de identificación (por ejemplo, licencia de conducción).

. • Número de identificación tributaria de la persona (NIT) (por ejemplo, el número de Seguro Social (SSN) o números de identificación del empleador (EIN en EE. UU.) o si éstos no están disponibles, el número de la cédula de extranjería o del pasaporte y país de expedición, o alguna anotación incluida en el registro indicando la ausencia de dicho(s) documento(s). Si el banco del originador sabe que la persona que coloca la orden de pago no es el originador, dicho banco del originador debe obtener y registrar el NIT del originador (por ejemplo, el número de Seguro Social o el EIN) o si éstos no están disponibles, el número de la cédula de extranjería o del pasaporte y país de expedición del mismo, o una anotación indicando la ausencia de dicho(s) documento(s).

Órdenes de pago no realizadas personalmente

Si la orden de pago no se hace personalmente, el banco del originador debe obtener y retener los siguientes registros:

. • Nombre y dirección de quien coloca la orden

. • El NIT o Número de identificación tributaria de la persona [TIN en EE. UU.] (por ejemplo, el número de Seguro Social (SSN) o número de identificación del empleador (EIN por su sigla en inglés, para EE. UU.) o, si no están disponibles, el número de la cédula de extranjería o del pasaporte y país de expedición, o una anotación el registro indicando la ausencia de dicho(s) documento(s), y una copia o registro del método de pago (por ejemplo, transacción efectuada con cheque o tarjeta de crédito). Si el banco del originador sabe que quien coloca la orden de pago no es el originador, dicho banco del originador debe obtener y registrar el NIT del originador (por ejemplo, el número de Seguro Social o el EIN) o, si éstos no están disponibles, el número de cédula de extranjería o del pasaporte y país de expedición del mismo, o una anotación indicando la ausencia de dicho(s) documento(s).

Recuperación de la información

La información retenida debe ser recuperable mediante referencia al nombre del originador. Cuando el originador es un cliente establecido del banco y dispone de una cuenta que utiliza para transferencias de fondos, la información retenida también debe ser recuperable por número de cuenta (31 CFR 103.33(e)(4)). Dichos registros deben mantenerse durante un período de cinco (5) años.

Requisito de la Regla para viajes

Para las transmisiones de fondos de US $ 3.000 o más, la entidad financiera del transmisor debe incluir la siguiente información en la orden de transmisión, en el momento en que dicha orden de transmisión se envía a la entidad financiera receptora (31 CFR

103.33(g)(1)):

. • Nombre del transmisor y, si el pago se ordena desde una cuenta, número de la cuenta del transmisor
. • Dirección del transmisor
. • Monto de la orden de transmisión
. • Identidad de la entidad financiera del receptor
• Los siguientes elementos, según el número que se reciba con la orden de transmisión:
– Nombre y dirección del receptor
– número de cuenta del receptor
– cualquier otra identificación específica del receptor

. • El nombre y la dirección o el identificador numérico de la entidad financiera del transmisor.

La Regla a la Viajes no dispone de requerimientos en cuanto a registros.

OBLIGACIONES DE LAS ENTIDADES INTERMEDIARIAS

Requerimientos en cuanto a registros

Por cada orden de pago por valor de US $3.000 o más que un banco acepte realizar como banco intermediario, dicho banco debe guardar un registro de la orden de pago.

Requisito de la Regla para viajes

Para las transmisiones de fondos de US $ 3.000 o más, la entidad financiera intermediaria debe incluir la siguiente información si se recibe de parte del remitente en una orden de transmisión en el momento en que en dicha orden se envía a la entidad financiera receptora (31 CFR 103.33(g)(2)):

. • Nombre y número de cuenta del transmisor
. • Dirección del transmisor
. • Monto de la orden de transmisión
. • Fecha de la orden de transmisión
. • Identidad de la entidad financiera del receptor
• Los siguientes elementos, según el número que se reciba con la orden de transmisión:
– Nombre y dirección del receptor
– Número de cuenta del receptor
– Cualquier otra identificación específica del receptor

. • El nombre y la dirección o el identificador numérico de la entidad financiera del transmisor.

Las entidades financieras intermediarias deben transmitir toda la información recibida de la entidad financiera del transmisor o la entidad financiera anterior, pero no están obligadas a obtener la información que no haya sido suministrada por la entidad financiera del transmisor o la entidad financiera anterior.

OBLIGACIONES DE LOS BANCOS DE LOS BENEFICIARIOS

Requerimientos en cuanto a registros

Si el beneficiario no es un cliente establecido del banco, la entidad del beneficiario debe retener la siguiente información por cada pago realizado por valor de US $3.000 o más.

Fondos a ser entregados personalmente

Si los fondos se entregan personalmente al beneficiario o a su representante o agente, la entidad debe verificar la identidad de la persona que recibe los fondos y conservar un registro con la siguiente información:

Nombre y dirección Tipo de documento revisado Número de identificación del documento Número de identificación tributaria (NIT) de la persona, o si éste no está disponible, número de la cédula de extranjería o del pasaporte y país de expedición, o una anotación en el registro indicando la ausencia de dicho(s) documento(s). Si la entidad sabe que la persona que recibe los fondos no es el beneficiario, debe obtener y conservar un registro del nombre y la dirección del beneficiario, así como de la identificación del beneficiario.

Fondos que no se entregan personalmente

Si los fondos no se entregan personalmente, la entidad debe retener una copia del cheque u otro instrumento empleado para efectuar el pago, o debe registrar la información relativa al instrumento. La entidad también debe registrar del nombre y la dirección de la persona a la cual éste ha sido enviado.

Recuperación

La información retenida debe ser recuperable por referencia al nombre del beneficiario. Si el beneficiario es un cliente establecido de la entidad y dispone de una cuenta empleada para las transferencias de fondos, la información retenida también debe ser recuperable por número de cuenta (31 CFR 103.33(e)(4)).

No existen requerimientos relativos a la Regla para Viajes para los bancos beneficiarios.

EXPIRACIÓN DE LA EXCEPCIÓN DEL ARCHIVO DE INFORMACIÓN CONDICIONAL DE LOS CLIENTES -REGLA PARA VIAJES

Entre 1998 y 2004, una excepción condicional a la Regla para viajes en términos generales le permitió a los bancos incluir un nombre codificado o seudónimo de cliente en las órdenes de transmisión, siempre y cuando el banco tuviera la información completa sobre el cliente en un archivo automatizado de información del cliente (CIF, por su sigla en inglés). FinCEN revocó esta excepción, conocida como la "excepción CIF", el 1º de julio de 2004. A partir de ésta fecha las entidades quedaron obligadas a utilizar el verdadero nombre y dirección de los clientes para poder cumplir con la Regla

ABREVIACIONES Y DIRECCIONES

Aunque la Regla para viajes no permite usar nombres codificados o seudónimos, sí permite usar nombres abreviados, nombres que reflejan distintas cuentas de una corporación (por ejemplo, Cuenta de Nómina de XYZ) y nombres comerciales o nombres adoptados para negocios (como por ej., “opera comercialmente bajo el nombre de”) o los nombres de las divisiones o departamentos que no están formalmente constituidos y que hacen parte del negocio.

Dirección del cliente

El término "dirección" tal como se emplea en (31 CFR 103.33(g) no está definido. Las directrices emitidas previamente por FinCEN han sido interpretadas como contrarias al uso de la dirección de correo en las órdenes de transmisión, cuando la entidad financiera del transmisor conoce la dirección. Sin embargo, en la notificación incluida en el Registro Federal del 28 de noviembre de 200368, FinCEN expidió una interpretación regulatoria que sostiene que la Regla para viajes debe permitir el uso de las direcciones de correo, incluyendo apartados aéreos [post office boxes], en el campo de dirección del transmisor de las órdenes de transmisión, en ciertas circunstancias.

La interpretación regulatoria sostiene que, para los fines de 31 CFR 103.33(g), el término "dirección" significa la dirección de correo del transmisor o la dirección del transmisor registrada en el archivo automatizado CIF de la entidad financiera (como por ejemplo una dirección de correo que incluye un número de apartado aéreo [post office box]), siempre y cuando la entidad tenga la dirección del transmisor69 en sus registros y dicha dirección sea recuperable mediante solicitud formulada por las autoridades.

[68] Ver el 68 Registro Federal 66708 en www.fincen.gov.

[69] De conformidad con las reglas definitivas expedidas en la sección 326 de la Ley Patriota, para los fines de la Regla para viajes una "dirección" significa lo siguiente: en el caso de una persona, una dirección residencial o comercial, un Apartado Aéreo del Ejército o Apartado Aéreo de Flota, o la dirección residencial o comercial del familiar más cercano u otra persona de contacto, para quienes no cuentan con una dirección residencial o comercial. Para quienes no son personas individuales (sino, por ejemplo, corporaciones, asociaciones o fideicomisos), la "dirección" consiste en la sede principal de negocios, oficina local u otra ubicación física. Sin embargo, si bien las reglas de la sección 326 aplican únicamente para nuevos clientes que han abierto cuentas a partir del 1 de octubre de 2003, y exceptúa las transferencias de fondos de la definición de "cuenta", en el caso de los bancos la Regla para viajes aplica a todas las transmisiones de fondos por valor de US $ 3.000 o más, sin importar si el transmisor es un cliente para los fines de las reglas de la sección 326.

Visión general fundamental – Registros de cuentas de corresponsalía extranjeras y debida diligencia

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios de cuentas de corresponsalía de bancos ficticios o bancos fachada extranjeros, registros de cuentas de corresponsalía extranjeras, y programas de debida diligencia para detectar y reportar el lavado de dinero y operaciones sospechosas. Favor referirse a las secciones ampliadas del manual para ver discusiones y procedimientos relativos a otros riesgos de lavado de dinero asociados a las cuentas de corresponsalía extranjeras.

VISIÓN GENERAL

Uno de los principales objetivos de la Ley Patriota ha sido el de proteger el acceso al sistema financiero de los Estados Unidos mediante el establecimiento de ciertos registros y programas de debida diligencia para cuentas corresponsales extranjeras. Además, la Ley Patriota prohíbe las cuentas de bancos ficticios extranjeros. Las cuentas de corresponsales extranjeros, tal como se observó en informes investigativos anteriores realizados por el Senado de los Estados Unidos[70], constituyen una puerta de ingreso al sistema financiero de ese país. Esta sección del manual cubre los requisitos regulatorios fijados en las secciones 312, 313 y 319(b) de la Ley Patriota y en las regulaciones de implementación establecidas en 31 CFR 103.177, 103.181 y 103.185. En las secciones ampliadas se incluyen discusiones y procedimientos adicionales sobre los riesgos específicos de lavado de dinero que atañen a las actividades de bancos corresponsales extranjeros, tales como actividades de transporte [o valija] de valores [pouch activities], cartas de efectivo, cheques en dólares de Estados Unidos y cuentas de quienes residen fuera de EE. UU. para efectuar pagos en EE. UU. [payable through accounts].

PROHIBICIÓN DE BANCOS FICTICIOS EXTRANJEROS Y REGISTROS DE LAS CUENTAS DE CORRESPONSALES EXTRANJERAS

El 28 de octubre de 2002 entró en vigencia la reglamentación definitiva (31 CFR 103.177 y 103.185) de las secciones 313 y 319(b) de la Ley Patriota. La reglamentación implementó nuevas disposiciones de la Ley del Secreto Bancario para cuentas de corresponsales extranjeros[71]. Bajo 31 CFR 103.177 se prohíbe a los bancos

[70] "La banca corresponsal: un portal para el lavado de dinero", ver la Sesión del Senado [de los Estados Unidos] Número 107-84. El informe aparece en la página 273 del volumen 1 del Acta de la Sesión, titulada "Papel de la banca corresponsal de Estados Unidos en el lavado de dinero internacional", celebrada el 1, 2 y 6 de marzo de 2001.

[71] Para los fines de 31 CFR 103.177 y 103.185, una "cuenta corresponsal" es una cuenta abierta en un banco para otro banco extranjero con el propósito de recibir depósitos y hacer pagos u otros desembolsos de dicho banco extranjero o en nombre del mismo, o para manejar otras transacciones financieras relativas a dicho banco extranjero. Una "cuenta" significa cualquier relación bancaria formal o relación de negocios establecida para prestar servicios, negociaciones y otras transacciones financieras corrientes, e

establecer, mantener, administrar o gerenciar cuentas de corresponsalía en Estados Unidos para bancos ficticios extranjeros o en nombre de los mismos. Los bancos ficticios extranjeros se definen como bancos extranjeros que no tienen presencia física en ningún país[72]. Como excepción, sin embargo, se permite a los bancos mantener cuentas de corresponsalía de bancos ficticios extranjeros que sean entidades afiliadas reguladas[73]. La sección 313 también requiere que los bancos adopten medidas razonables para asegurar que las cuentas de corresponsalía de bancos extranjeros no sean utilizadas para suministrar servicios bancarios indirectos a los bancos ficticios extranjeros.

Certificaciones

Los bancos que tengan cuentas de corresponsalía de bancos extranjeros en Estados Unidos deben tener registros en Estados Unidos con la identificación de los propietarios de cada banco extranjero[74]. Deben también tener registrado el nombre y la dirección de la persona que reside en Estados Unidos autorizada para actuar como agente, a quien puede notificarse oficialmente sobre procesos jurídicos[75]. Bajo 31 CFR 103.185, los bancos deben producir estos registros a los siete (7) días de recibir una notificación escrita de parte de autoridades federales en la cual se solicitan dichos registros.

La Tesorería de los Estados Unidos, trabajando conjuntamente con la industria y las autoridades y agencias bancarias federales, ha desarrollado un "proceso de certificación" para ayudarle a los bancos a cumplir con las disposiciones sobre registros. Este proceso incluye formularios de certificación y re-certificación. Si bien los bancos

incluye transacciones o cuentas de depósito de demanda, depósito de ahorros u otras transacciones o cuentas de activos así como una cuenta de crédito y otras extensiones de crédito (31 103.175(d)).

[72] La "presencia física" significa una sede de negocios que:

. • es mantenida por un banco extranjero
. • está ubicada en una dirección fija (distinta a una dirección meramente electrónica o apartado aéreo postal) en un país en el cual la entidad financiera extranjera está autorizada para realizar

actividades bancarias, y en cuya ubicación dicha entidad financiera extranjera: – emplea a una o más personas de tiempo completo – mantiene registros operativos relacionados con sus actividades bancarias
. • está sujeta a inspección por parte de las autoridades bancarias que autorizaron a dicha entidad financiera extranjera realizar actividades bancarias.

[73] Una "afiliada regulada" es un banco ficticio que está afiliado a una entidad de depósito [depositary institution] cooperativa de crédito [credit union] o banco extranjero que mantiene presencia física en los Estados Unidos o en alguna otra jurisdicción. El banco ficticio afiliado regulado también debe estar sujeto a la supervisión de las autoridades bancarias que regulan a la entidad afiliada.

[74] Para minimizar la carga relativa al mantenimiento de registros, no es necesario guardar la información sobre propiedad en el caso de entidades financieras extranjeras que radican el formulario FR Y-7 (“Reporte anual de organizaciones bancarias extranjeras") ante la Reserva Federal o en el de las entidades financieras extranjeras que se transan públicamente [que cotizan públicamente en la bolsa]. “Transarse públicamente” [cotizarse públicamente en la bolsa] se refiere a las acciones que se cotizan en una bolsa o en un mercado organizado sobre el mostrador [over-the-counter market] regulado por alguna autoridad de títulos valores extranjera, según la definición que aparece en la sección 3(a)(50) de la Ley de la Bolsa de Valores de 1934.

“Notificarse oficialmente sobre procesos jurídicos” significa que el agente está dispuesto a aceptar documentos jurídicos, tales como citaciones, en nombre del banco extranjero.
no están obligados a usar estos formularios, se considerará que los bancos "cumplen" con el reglamento si cuentan con un formulario de certificación debidamente diligenciado por la entidad financiera extranjera y obtienen la re-certificación una vez cada tres (3) años.

Cierre de cuentas

La regulación a su vez incluye disposiciones específicas sobre el momento en que los bancos deben obtener la información requerida o, de lo contrario, cerrar las cuentas de corresponsalía. Los bancos deben obtener la certificación (o re-certificación) o la información requerida dentro de los treinta (30) días calendario siguientes a la fecha en que se abre la cuenta, y al menos una (1) vez cada tres (3) años de ahí en adelante. Si no logra obtener la información requerida, el banco debe proceder a cerrar todas las cuentas de corresponsalía de bancos extranjeros en un plazo de tiempo comercialmente razonable.

Verificación

Los bancos deben revisar la razonabilidad y precisión de las certificaciones. Si en cualquier momento un banco sabe, sospecha o tiene razones para sospechar que la información que contiene alguna certificación (o re-certificación) o cualquier otra información que le haya sido suministrada ya no es válida, debe solicitarle al banco extranjero verificar o corregir dicha información o adoptar otras medidas apropiadas para determinar la precisión de la misma. Por lo tanto es necesario revisar las certificaciones para verificar posibles problemas que ameriten mayor revisión, tales como el uso de direcciones de apartado aéreo postal [post office boxes] o direcciones de terceros para remisión. Si transcurridos noventa (90) días el banco no ha obtenido la información requerida o no ha corregido la información, se debe proceder a cerrar la cuenta en un plazo de tiempo comercialmente razonable. Durante dicho periodo el banco no le permitirá al banco extranjero establecer ninguna posición financiera nueva ni ejecutar transacción alguna a través de la cuenta,

distinta a las que se requieran para cerrar la cuenta. Además, el banco no podrá abrirle ninguna otra cuenta de corresponsalía a dicho banco extranjero sino hasta cuando haya obtenido la información requerida.

Los bancos también deben retener la copia original de los documentos suministrados por el banco extranjero y la copia original de cualquier otro documento utilizado para los fines de la regulación, durante un mínimo de cinco (5) años siguientes a la fecha a partir de la cual el banco ya no tiene más cuentas de corresponsalía del banco extranjero.

Citaciones judiciales

Bajo la sección 319(b) de la Ley Patriota, el Secretario del Tesoro o el Fiscal General de los Estados Unidos pueden expedir citaciones judiciales a cualquier banco extranjero que tenga cuentas de corresponsalía en Estados Unidos, con el fin de obtener registros relativos a dicha(s) cuenta(s), incluyendo registros que se mantienen en el exterior, o para obtener registros relativos al depósito de fondos en el banco extranjero. Si el banco [de EE. UU.] incumple la citación judicial o no inicia procedimientos para dar respuesta a la misma, el Secretario del Tesoro o el Fiscal General de los Estados Unidos (luego de realizar consultas mutuas) podrán ordenarle, mediante notificación escrita, que termine su relación con el banco corresponsal extranjero. Si para el décimo (10º) día siguiente al recibo de dicha notificación el banco incumple la orden de dar por terminada su relación de corresponsalía, podrá incurrir en una sanción monetaria civil de hasta US $10.000 diarios hasta el día en que efectivamente de por terminada la relación de corresponsalía.

Solicitud de registros AML (Anti-lavado de dinero) del Regulador Federal

Igualmente, mediante solicitud formulada por su [respectivo] regulador federal, los bancos están obligados a suministrar sus registros relativos al cumplimiento del banco o de sus clientes con la Lucha contra el Lavado de Dinero , dentro de las ciento veinte (120) horas siguientes a la formulación de la solicitud.

PROGRAMA ESPECIAL DE DEBIDA DILIGENCIA PARA CUENTAS CORRESPONSALES EXTRANJERAS

La sección 312 de la Ley Patriota agregó el nuevo literal (i) a 31 USC 5218 de la Ley del Secreto Bancario. Esta sección requiere que todo banco de EE. UU. que establezca, mantenga, administre o gerencie una cuenta de corresponsalía en EE. UU. en nombre de una persona que no es de EE. UU., adopte ciertas medidas de Lucha contra el Lavado de Dinero respecto a dichas cuentas. Particularmente los bancos deben establecer políticas, procedimientos y procesos de debida diligencia apropiados, específicos y donde sea necesario, mejorados, razonablemente diseñados para que el banco pueda detectar y reportar instancias de lavado de dinero a través de dichas cuentas. Este requisito aplica para toda relación de corresponsalía con cualquier entidad financiera extranjera, aún si no se

trata de una entidad bancaria tradicional. Además de este requisito general, que aplica para todas las cuentas corresponsales de quienes no sean ciudadanos de EE.UU., la sección 312 de la Ley Patriota especifica normas adicionales para las cuentas de corresponsalía de ciertos bancos extranjeros. Para las cuentas de corresponsalía de bancos extranjeros que operan bajo licencias extraterritoriales o licencias otorgadas por jurisdicciones que han sido designadas como motivo de preocupación con respecto al lavado de dinero, los bancos deben adoptar medidas razonables para identificar a los propietarios de la entidad financiera extranjera, examinar cuidadosamente la cuenta de corresponsalía para salvaguardarse contra el lavado de dinero, verificar si el banco extranjero tiene cuentas de corresponsalía con otros bancos extranjeros, y si ese es el caso, realizar una debida diligencia apropiada.

Regla definitiva interina

El 23 de julio de 2002 el Departamento del Tesoro de los Estados Unidos informó por medio del *Registro Federal* que no sería posible completar la regla definitiva de implementación de la sección 312 para la fecha establecida estatutariamente del 23 de julio de 2002[76]. Por lo tanto el Tesoro de los Estados Unidos publicó una regla definitiva interina que pospuso la aplicación de las disposiciones de debida diligencia a las cuentas de corresponsalía de la sección 5318(i) de entidades financieras no bancarias. Por lo tanto, los bancos deben cumplir con la sección 5318(i) hasta que la Tesorería expida la reglamentación definitiva. La regla definitiva interina que aplica

[76] Ver el 67 Registro Federal 48348 en www.fincen.gov.

para los bancos está promulgada en 31 CFR 103.181[77]. El preámbulo de la notificación que apareció en el *Registro Federal* publicado con la regla definitiva interina sirve de guía para las entidades financieras, incluyendo a los bancos, con respecto a los cuales no se ha diferido la sección 5318(i). Dicho literal 5318(i) aplica para todas las cuentas, sin importar el momento en que se hayan abierto.

Desde una perspectiva práctica, los bancos no podrán diseñar e implementar políticas y procedimientos integrales y definitivos de debida diligencia, de conformidad con lo ordenado por 31 CFR 5318(i), sino hasta cuando el Tesoro de los Estados Unidos expida la reglamentación definitiva. Mientras tanto, los examinadores se deben enfocar en las políticas, procedimientos y procesos de los bancos para el cumplimiento de las dos (2) disposiciones básicas establecidas en 31 USC 5318(i) en relación con la banca corresponsal:

. • Debida diligencia de tipo general para las cuentas de corresponsalía que se mantienen para todas las entidades financieras extranjeras (31 USC 5318(i)(1)), y
. • Debida diligencia mejorada para las cuentas de corresponsalía que se mantienen para ciertos bancos (31 USC 5318(i)(2)).

FinCEN y las agencias bancarias federales esperan que, una vez el Departamento del Tesoro de los Estados Unidos expida la regla definitiva, los procedimientos de examen revisados se desarrollen mediante un esfuerzo conjunto de las agencias.

Debida diligencia general

El numeral 5318(i)(1) requiere que los bancos fijen políticas, procedimientos y controles de debida diligencia diseñados en forma razonable para detectar y reportar el lavado de dinero a través de cuentas corresponsales establecidas, mantenidas, administradas o gerenciadas en Estados Unidos para entidades financieras extranjeras. Mientras tanto, el programa de debida diligencia según el numeral 5318(i)(1) podrá considerarse razonable si establece políticas, procedimientos y procesos de evaluación de los riesgos que plantean las cuentas de corresponsalía extranjeras, y dirige los esfuerzos de cumplimiento a las cuentas corresponsales que representan alto riesgo de lavado. El preámbulo de la notificación publicada en el *Registro Federal* conjuntamente con la regla definitiva interina estableció que, al realizar la debida diligencia, los bancos deben darle prioridad a:

. • Las entidades financieras extranjeras de alto riesgo para las que tienen cuentas de depósito de corresponsalía o equivalentes.
. • Las cuentas de corresponsalía utilizadas para prestarle a terceros.
. • Las cuentas de corresponsalía de alto riesgo de entidades financieras extranjeras no bancarias, tales como transmisores de dinero [money transmitters].

Para la reglamentación definitiva interina especificada en 31 CFR 103.181, una cuenta de corresponsalía es una cuenta establecida para recibir depósitos de una entidad financiera extranjera, hacer pagos en nombre de dicha entidad o manejar otras transacciones financieras relacionadas con la misma. Una cuenta significa cualquier relación bancaria formal o de negocios establecida para suministrar servicios, negociaciones u otras transacciones financieras regulares, e incluye un depósito de demanda, depósitos de ahorros u otra cuenta para transacciones o activos así como una cuenta de crédito u otra extensión de crédito (31 USC 5318A(e)).

Mientras tanto, una política razonable de debida diligencia debe cumplir con las buenas prácticas y estándares que aplican para los bancos que tienen cuentas de corresponsalía de entidades financieras extranjeras. Dicha política debe evidenciar los esfuerzos de buena fe realizados por el banco para incorporar procedimientos de debida diligencia a las cuentas de corresponsalía de entidades financieras extranjeras que mantiene y que pueden representar un mayor riesgo de lavado de dinero.

Como ejemplos de buenas prácticas y estándares bancarios se pueden mencionar los siguientes:

. • The New York Clearing House Association, L.L.C. [empresa cuyo nombre traducido sería Asociación de Cámara de Compensación de Nueva York], “The New Cork Clearing House Issues Anti-Money Laundering Guidelines for Correspondent Banking”[“La Cámara de Compensación de Nueva York expide Guías de lucha contra el lavado de dinero para la banca corresponsal”] (marzo de 2002), en www.nych.org.
. • El Comité de Basilea de Supervisión Bancaria, “Customer Due Dilligence for Banks” ["Debida diligencia del cliente para bancos"] (octubre de 2001), en www.bis.org.

Es posible que un programa de debida diligencia que no incluya todas las buenas prácticas y estándares que han sido descritas en la industria así como otras guías que están disponibles sea considerado como un programa razonable, si el banco respectivo puede

justificar no haber adoptado alguna buena práctica o estándar en particular debido al tipo particular de cuentas que tiene.

Evaluación de riesgo de las entidades financieras extranjeras

El programa general de debida diligencia de los bancos debe incluir políticas, procedimientos y procesos para evaluar los riesgos que representan los clientes que son entidades financieras extranjeras. Los recursos de un banco están mejor empleados cuando se enfocan en las cuentas que representan mayor riesgo de lavado de dinero. Los siguientes factores pueden ayudar a identificar las características que representan un riesgo potencial en los clientes de corresponsalía extranjeros. Sin embargo, la gerencia debe ponderar y evaluar cada factor de riesgo y generar una determinación de riesgo para cada cliente, para luego fijar prioridades entre los recursos de vigilancia y supervisión. Entre los factores de riesgo relevantes se pueden citar los siguientes:

. • La jurisdicción de la organización, constitución y licencia de la entidad financiera extranjera.
. • Los productos y servicios que ofrece la entidad financiera extranjera.
. • Los mercados (incluyendo la base de clientes) y ubicaciones que atiende la entidad financiera extranjera.
. • La finalidad de la cuenta (por ejemplo, cuenta para operaciones exclusivas [proprietary operating account] o cuenta dirigida por el cliente [customer-directed account].
. • Actividades anticipadas (por ejemplo, monto en dólares, número y tipos de transacciones) de la cuenta.
. • La naturaleza y duración de la relación que tiene el banco con la entidad financiera extranjera (y si aplica, con cualquier afiliada de dicha entidad financiera extranjera).
. • Cualquier información que conozca el banco o que se encuentre razonablemente a su alcance relativa al desempeño de la entidad financiera extranjera en la lucha contra el lavado de dinero, incluyendo información de dominio público disponible en guías, publicaciones periódicas y publicaciones principales generales de la industria.

Debida diligencia mejorada para ciertos bancos extranjeros

El numeral 5318(i)(2) requiere que los bancos establezcan políticas y procedimientos de debida diligencia mejorada al abrir o mantener cuentas de corresponsalía en los Estados Unidos solicitadas por ciertos bancos extranjeros o en el nombre de éstos o que éstos mantengan bajo las siguientes modalidades:

. • Con licencia bancaria extraterritorial[78].
. • Con licencia bancaria expedida por un país extranjero calificado como país no cooperante con los principios o procedimientos internacionales de lucha contra el lavado de dinero por parte de algún grupo u organización intergubernamental de la cual Estados Unidos es miembro, y con cuya designación está de acuerdo el representante de los Estados Unidos ante dicho grupo u organización.
• Con licencia bancaria expedida por un país extranjero calificado por el

Secretario del Tesoro [de EE. UU.] como país que amerita medidas especiales debido a la posibilidad de lavado de dinero.

Según los literales 5318(i)(2)(b)(i) hasta el (iii), los bancos deben establecer políticas, procedimientos y controles para asegurar que por cada banco extranjero así sujeto a la debida diligencia mejorada, los bancos adopten medidas razonables dirigidas a:

. • Determinar, por cada banco extranjero de este tipo cuyas acciones no se coticen públicamente en la bolsa, la identidad de cada uno de los propietarios de dicho banco extranjero, así como la naturaleza y el tipo de propiedad que posee cada propietario[79].

. • Realizar un examen detallado de todas las cuentas que posee dicho banco para salvaguardarse contra el lavado de dinero y reportar toda transacción sospechosa, de conformidad con las regulaciones relativas a los ROS.

. • Determinar si dicho banco extranjero ofrece cuentas de corresponsalía a otros bancos extranjeros, y de ser éste el caso, determinar la identidad de dichos bancos extranjeros y realizar la debida diligencia según corresponda según los requerimientos fijados en el numeral 5318(i)(1) (por ejemplo, el programa general

La Ley Patriota define la licencia bancaria extraterritorial como una licencia para la realización de actividades bancarias que, como condición de la licencia, le prohíbe a la entidad que recibe la licencia realizar actividades bancarias con ciudadanos del país que expide la licencia o en la moneda local del mismo. Ver 31 USC 5318(i)(4)(A).

[79] El preámbulo de la notificación publicada en el *Registro Federal* conjuntamente con la regla definitiva interina (67 *Registro Federal* 48348) afirmó que para los fines del literal 5318(i)(2)(B)(i.), se considera que un propietario es cualquier persona que sea directa o indirectamente propietaria o controle o tenga poder de voto sobre el 5% o más de los valores de cualquier tipo de un banco extranjero cuyas acciones no se coticen en la bolsa. "Cotizarse [transarse] públicamente en la bolsa" ["publicly traded"] se refiere a acciones que se transan en una bolsa o mercado organizado "sobre el mostrador" [over the counter] regulado por alguna autoridad de títulos valores extranjera, según lo que se define en la sección 3(a)(50) de la Ley de Títulos Valores de 1934 (15 USC 78c(a)(50)).

de debida diligencia del banco). Tomando en cuenta factores de riesgo tales como la localización y tamaño del banco corresponsal extranjero y el número de sus clientes que son entidades financieras extranjeras, el banco debe determinar el grado hasta el cual es necesaria la debida diligencia de los clientes que son entidades financieras extranjeras del banco corresponsal extranjero.

Los bancos deben dirigir sus medidas de debida diligencia mejorada a las cuentas de corresponsalía que mantienen los bancos extranjeros que, según 31 USC 5318(i)(2)(A) representan un riesgo significativamente alto de lavado de dinero sobre la base de la evaluación general del riesgo que representa el banco extranjero. Además, los bancos deben aplicar cualquiera de los pasos anotados arriba, o la totalidad de los mismos, según sea apropiado, a la entidad financiera extranjera que ha sido identificada por el programa de debida diligencia general del banco como entidad que representa un mayor riesgo de lavado de dinero.

Visión general fundamental – Programa de debida diligencia de la banca privada (para quienes no son ciudadanos de EE. UU.)

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios dirigidos a implementar políticas, procedimientos y controles para detectar y reportar el lavado de dinero y actividades sospechosas realizadas a través de cuentas bancarias privadas establecidas, administradas o mantenidas en nombre de personas que no son de EE. UU. Ver las secciones ampliadas del manual para conocer discusiones y procedimientos relativos a otros riesgos de lavado de dinero que están asociados a la banca privada.

VISIÓN GENERAL

La banca privada puede definirse en términos generales como [el conjunto de] los servicios financieros personalizados que se ofrecen a los clientes adinerados. La Ley Patriota enmendó la Ley del Secreto Bancario y definió la "cuenta bancaria privada" como una cuenta o combinación de cuentas que cumple con los siguientes criterios:

. • Requiere un mínimo de fondos agregados u otros activos por un valor no inferior a US $ 1 millón.
. • Se establece en nombre de una o más personas que tiene(n) interés directo como propietario(s) o usufructuario(s) de la cuenta.
. • Está parcial o completamente asignada a un funcionario, empleado o agente de la entidad financiera o es administrada por aquel, quien actúa como enlace entre la entidad financiera y el propietario o beneficiario directo de la cuenta[80].

La sección 312 de la Ley Patriota agregó un nuevo literal (i) a 31 USC 5318 de la Ley del Secreto Bancario. Esta sección requiere que toda entidad financiera de Estados Unidos que abra, mantenga, administre o gerencia una cuenta bancaria privada en los Estados Unidos (según la definición anotada arriba) para personas que no son de Estados Unidos, adopte ciertas medidas de lucha contra el lavado de dinero con respecto a dicha cuenta. En particular los bancos deben establecer políticas, procedimientos y controles de debida diligencia apropiados, específicos y donde sea necesario, mejorados, razonablemente diseñados para permitirle a los bancos detectar y reportar instancias de lavado de dinero efectuado a través de cuentas bancarias privadas establecidas, administradas o mantenidas en los Estados Unidos para personas que no son de Estados Unidos. Además de este requerimiento general, la sección 312 fija estándares mínimos para las cuentas bancarias privadas solicitadas o mantenidas por personas que no son de Estados Unidos o en nombre de las mismas, para asegurarse que, como mínimo, los bancos adopten medidas razonables dirigidas a:

[80] Ver el literal 31 USC 5318(i)(4)(B). Esta definición específica que la "cuenta bancaria privada" aplica únicamente para los requerimientos de la debida diligencia especial según 31 USC 5318(i.).

- Determinar la identidad de los propietarios nominales y beneficiarios así como el origen de los fondos depositados en las cuentas bancarias privadas, según se requiera para salvaguardarse contra el lavado de dinero y para reportar cualquier transacción

sospechosa.

- Realizar un examen cuidadoso de toda cuenta bancaria privada solicitada o mantenida por políticos extranjeros de alto nivel o en nombre suyo, o por cualquier miembro de la familia inmediata o asociado cercano a personalidades políticas extranjeras de alto nivel (también conocidos como personas políticamente expuestas (PEP por su sigla en inglés)). Este examen detallado está razonablemente diseñado para detectar y reportar transacciones que puedan incluir fondos provenientes de corrupción ocurrida en el extranjero[81].

La visión general y los procedimientos incluidos en esta sección tienen la finalidad de evaluar el programa de debida diligencia del banco relativo a las cuentas bancarias privadas ofrecidas a personas que no son de los Estados Unidos. En la sección de procedimientos de examen ampliados titulada "Banca privada" de la página 253 se incluyen procedimientos adicionales relativos a ciertas áreas concretas de riesgo inherentes a la banca privada.

Regla definitiva interina

El 23 de julio de 2002 el Departamento del Tesoro de los Estados Unidos dio a conocer por medio del *Registro Federal* que no sería posible completar razonablemente la regla definitiva de implementación de la sección 312 para la fecha establecida estatutariamente del 23 de julio de 2002[82]. Por lo tanto el Tesoro de los Estados Unidos publicó una regla definitiva interina que pospuso la aplicación de las disposiciones sobre banca privada de la sección 5318(i) a las entidades financieras no bancarias, agentes y corredores de valores, comisionistas del mercado de futuros, e introduciendo a los agentes / intermediarios. Por lo tanto, los bancos deben cumplir con la sección 5318(i) hasta que la Tesorería expida la regla definitiva. La regla definitiva interina que aplica para los bancos está promulgada en 31 CFR 103.181[83]. El preámbulo de la notificación que apareció en el *Registro Federal* publicado con la regla definitiva interina sirve de guía a las entidades financieras para las cuales no se ha diferido la sección 5318(i), lo que incluye a los bancos. Dicho literal 5318(i) aplica para todas las cuentas, sin importar el momento en que se hayan abierto.

Desde una perspectiva práctica, los bancos no podrán diseñar e implementar políticas y procedimientos y controles integrales y definitivos de debida diligencia, de conformidad con lo ordenado por el literal 5318(i), sino hasta cuando el Tesoro de los Estados Unidos expida la reglamentación definitiva. FinCEN y las agencias bancarias federales esperan que sea posible desarrollar los procedimientos de examen revisados mediante

[81] Ver la sección ampliada sobre procedimientos titulada "Personas políticamente expuestas" en la página 259.

[82] Ver el 67 Registro Federal 48348 en www.fincen.gov.

Para los propósitos de la regla definitiva interina, el término "banco" incluye: bancos, entidades de ahorro y crédito [thrifts], asociaciones de ahorro, cooperativas de crédito [credit unions], organizaciones bancarias extranjeras (FBO por su sigla en inglés) y corporaciones relativas a la Ley Edge así como “agreement corporations”.

DEBIDA DILIGENCIA

Un programa de debida diligencia bancaria privada debe estar diseñado de manera que permita razonablemente detectar y reportar el lavado de dinero y la existencia de fondos derivados de instancias de corrupción ocurridas en el extranjero. Mientras tanto, una política de debida diligencia razonable es una que (i) se compagina con las buenas prácticas y estándares actuales que aplican para los bancos que tienen cuentas bancarias privadas de personas que no son de los Estados Unidos, (ii) evidencia esfuerzos de buena fe dirigidos a incorporar los estándares mínimos de debida diligencia descritos arriba, y (iii) se enfoca en las cuentas bancarias privadas que representan un alto riesgo de lavado de dinero. Entre los ejemplos de buenas prácticas y estándares se pueden mencionar los siguientes:

. • La Junta de Gobernadores del Sistema de la Reserva Federal, "Actividades bancarias privadas" (SR carta 97-19 (SUP), 30 de junio de 1997) en www.federalreserve.gov.

. • Departamento del Tesoro de los Estados Unidos, reguladores bancarios federales, y el Departamento de Estado de los Estados Unidos, "Guía de seguridad aumentada para las transacciones que pueden incluir fondos derivados de instancias de corrupción ocurrida en el extranjero", (enero de 2001) en www.treas.gov/press/releases/docs/guidance.htm.

. • El Grupo Wolfsberg, “Principios Wolfsberg contra el lavado de dinero en la banca privada” (primera revisión, mayo de 2002) en www.wolfsberg-principles.com.

. • Banco de Pagos Internacionales (BPI) [Bank for Internacional Settlements – BIS], Comité de Supervisión Bancaria de Basilea, "Debida diligencia del cliente para bancos" (octubre de 2001) en www.treas.gov/press/releases/docs/guidance.htm.

Es posible que un programa de debida diligencia que no adopte todas las buenas prácticas y estándares descritos en las guías para el gobierno y la industria anotadas previamente, llegue ser considerado razonable. La entidad respectiva debe ser capaz de justificar no haber adoptado una buena práctica o norma en particular, con base en el tipo particular de cuentas que tiene.

Evaluación de riesgo de las cuentas bancarias privadas de personas que no son de los Estados Unidos

Los bancos deben desarrollar políticas, procedimientos y procesos de evaluación del riesgo que representan las cuentas bancarias privadas de personas que no son de los Estados Unidos, y dirigir sus recursos apropiadamente hacia las cuentas que impliquen mayor riesgo de lavado de dinero. Los siguientes factores pueden emplearse para identificar características de riesgo potencial entre los clientes de banca privada. Sin embargo, la gerencia debe ponderar y evaluar cada factor de riesgo para determinar el riesgo que implica cada cliente. Entre los factores de riesgo que son relevantes se encuentran los siguientes:

• La naturaleza del negocio del cliente (es decir, el origen de su riqueza). El tipo de negocio al que se dedica el cliente de la banca privada, el origen de la riqueza de

dicho cliente y el grado hasta el cual la historia comercial del cliente incrementa el riesgo de lavado de dinero. Se debe considerar este factor en el caso de cuentas bancarias privadas de políticos extranjeros de alto nivel, hasta donde sea necesario, para permitir la detección y el reporte razonables de transacciones que puedan involucrar fondos derivados de instancias de corrupción ocurridas en el extranjero.

. • El propósito de la cuenta y las actividades anticipadas. El tamaño, propósito, tipo de cuentas involucradas en la relación y las actividades esperadas con respecto a la cuenta (por ejemplo, montos en dólares y número y tipos de transacciones).

. • Historial del cliente. La naturaleza y duración de la relación del banco con el cliente de la banca privada.

. • Jurisdicción. La ubicación del domicilio y negocio del cliente de la banca privada. Esta revisión incluiría una consideración sobre el grado hasta el cual la jurisdicción relevante es reconocida a nivel internacional como una que presenta mayor riesgo de lavado de dinero, o por el contrario, una que dispone de normas de lucha contra el lavado de dinero más sólidas.

. • Información disponible. Cualquier información que conozca o que razonablemente pueda conocer la institución sobre el cliente de la banca privada. El alcance y la profundidad de dicha revisión dependerá de la naturaleza de la información que se pueda descubrir.

Visión general fundamental – Medidas especiales

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios de las medidas especiales emitidas en la sección 311 de la Ley Patriota.

VISIÓN GENERAL

La sección 311 de la Ley Patriota agregó 31 USC 5318 a la Ley del Secreto Bancario (BSA), y autoriza al Secretario del Tesoro a requerir de las instituciones financieras nacionales y agencias financieras nacionales tomar ciertas medidas especiales contra las jurisdicciones extranjeras, instituciones financieras extranjeras, clases de transacciones internacionales, o tipos de cuentas con potencial de lavado de dinero. La sección 311 le brinda al Secretario del Tesoro un rango de opciones que pueden adaptarse para dirigirse hacia aspectos específicos del lavado de dinero y la financiación del terrorismo. La sección 311 se implementa a través de diferentes órdenes y regulaciones que están incluidas en CFR Parte 103.[84] Como se consigna en la sección 311, se pueden imponer ciertas medidas especiales mediante una orden sin previa notificación pública o comentarios, pero dichas órdenes deben tener una vigencia limitada y deben emitirse conjuntamente con una Notificación de propuesta de reglamentación [Notice of Proposed Rulemaking].

La sección 311 establece un proceso que debe seguir el Secretario del Tesoro e identifica agencias federales que deben consultarse antes de que el Secretario pueda concluir que una jurisdicción, institución financiera, clase de transacciones, o tipo de cuenta tienen una alta posibilidad de lavado de dinero. El estatuto también dispone procedimientos similares, incluyendo factores y requerimientos de consulta, para seleccionar las medidas especiales específicas que se impondrán contra una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta con alta probabilidad de lavado de dinero.

Es importante anotar que, si bien una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta pueden designarse como de alta probabilidad de lavado de dinero en una orden emitida conjuntamente con la Notificación de propuesta de reglamentación [Notice of Proposed Rulemaking], las medidas especiales de duración ilimitada únicamente pueden imponerse mediante reglamentación definitiva emitida después de la Notificación y de una oportunidad que se ofrece para hacer comentarios.

TIPOS DE MEDIDAS ESPECIALES

Las notificaciones de las reglas propuestas y definitivas que acompañan el enunciado "de alta probabilidad de lavado de dinero" y la imposición de una medida (o medidas) especial(es) conforme a la sección 311 de la Ley Patriota se encuentran disponibles en el sitio web de FinCEN en www.fincen.gov.

Registros e informes de ciertas transacciones financieras

Bajo la primera medida especial los bancos pueden estar obligados a mantener o radicar informes sobre el número acumulado de transacciones o los datos específicos de cada transacción con respecto a una jurisdicción, institución financiera, clase de transacciones o tipo de cuenta con alta probabilidad de lavado de dinero. El estatuto fija unos requerimientos mínimos de información para estos registros e informes y permite que el Secretario del Tesoro imponga requerimientos adicionales respecto a la información.

Información relacionada a la titularidad

Bajo la segunda medida especial, los bancos pueden estar obligados a tomar medidas prácticas y razonables, según lo determine el Secretario del Tesoro, para obtener y retener información relativa a la titularidad de las cuentas que abra o tenga en los Estados Unidos una persona extranjera (diferente a una entidad extranjera cuyas acciones están sujetas a requerimientos de informes públicos o se cotizan y transan en una bolsa o mercado de intercambio regulado), o un representante de dicha persona extranjera, que incluya a una jurisdicción, entidad financiera, clase de transacciones o tipo de cuenta con alta probabilidad de lavado de dinero.

Información relacionada con ciertas cuentas utilizadas para pagos [Payable Through

Accounts]

Bajo la tercera medida especial, los bancos que abren o mantienen una cuenta utilizada para pagos [payable through account] relativa a una jurisdicción, entidad financiera, clase de transacción o tipo de cuenta con alta probabilidad de lavado de dinero, pueden estar sujetos a lo siguiente: (i) identificar a cada cliente (y representante) a quien se le permite utilizar la cuenta o cuyas transacciones se encausan a través de la cuenta; y (ii) obtener información sobre cada uno de dichos clientes (y representantes) básicamente similar a la que obtiene una entidad de depósitos [depositary institution] de los Estados Unidos en el curso normal de sus negocios con respecto a sus clientes que residen en los Estados Unidos[85].

Información relacionada con ciertas cuentas corresponsales

Bajo la cuarta medida especial, los bancos que abren y mantienen una cuenta corresponsal en los Estados Unidos relativa a una jurisdicción, entidad financiera, clase de transacción o tipo de cuenta con alta probabilidad de lavado de dinero, pueden estar sujetos a lo siguiente: (i) identificar a cada cliente (y representante) al que se le permite utilizar la cuenta o cuyas transacciones se encausan a través de la cuenta, y (ii) obtener información acerca de cada uno de estos clientes (y representantes) sustancialmente comparable a la que obtiene una institución de depósito de los Estados Unidos en el

[85] Ver la sección de visión general ampliada titulada “Cuentas para pagos” [Payable Through Accounts] en la página 102 para una mayor orientación.

Prohibiciones o condiciones para abrir o mantener ciertas cuentas corresponsales o cuentas usadas para realizar pagos

Bajo la quinta y más fuerte medida especial, puede prohibírsele a los bancos abrir o mantener cuentas corresponsales o cuentas usadas para realizar pagos [payable through accounts], para entidades financieras extranjeras o en nombre de las mismas, si la cuenta tiene relación con una jurisdicción, institución financiera, clase de transacciones,
o tipo de cuenta de alta probabilidad de lavado de dinero. Esta medida puede prohibirle a los bancos de Estados Unidos establecer, mantener, administrar o manejar cuentas corresponsales o de realización de pagos [payable through] para entidades financieras extranjeras o en nombre de las mismas, de una jurisdicción específica extranjera. Esta medida también puede cubrir a entidades financieras extranjeras específicas y sus sucursales.

Las regulaciones que implementan estas prohibiciones pueden requerir que los bancos revisen sus registros de cuentas para determinar que no mantienen cuenta directamente para dichas entidades o en nombre de las mismas. Además de la prohibición directa, a los bancos también se les puede exigir lo siguiente:

. • Sujetarse a la prohibición de suministrar conscientemente acceso indirecto a

las entidades específicas a través de sus demás relaciones bancarias.

. • Informar a los titulares de las cuentas corresponsales que no deben permitirle a la entidad específica acceso a la cuenta que se tiene en un banco de EE. UU.

. • Adoptar medidas razonables para identificar cualquier uso indirecto de sus cuentas por la entidad específica.

GUÍA DE MEDIDAS ESPECIALES

Las órdenes y regulaciones que implementan medidas específicas especiales adoptadas bajo la sección 311 de la Ley Patriota no son estáticas; pueden ser emitidas o revocadas a medida que el Secretario del Tesoro determina que una jurisdicción, institución, clase de transacciones o tipo de cuenta de una persona ya no se considera de alta probabilidad de lavado de dinero. Además, las medidas especiales impuestas contra una jurisdicción, institución, clase de transacciones o tipo de cuenta pueden variar con respecto a las que se imponen en otras situaciones. Los examinadores deben observar también que el cumplimiento con las medidas especiales no es necesariamente absoluto; una orden o regla que impone una medida especial puede establecer un estándar de debida diligencia que los bancos deben aplicar para cumplir con la medida especial específica.

Por consiguiente este manual no detalla medidas especiales definitivas, puesto que cualquier listado de este tipo prontamente se vería desactualizado. Los examinadores que revisan el cumplimiento de esta sección deben visitar el sitio web de FinCEN en www.fincen.gov para obtener información actualizada sobre las medidas especiales definitivas. Los examinadores deben llevar a cabo su examen con base en las medidas

Para obtener mayor orientación ver la sección de visión general fundamental titulada “Registros y debida diligencia de las cuentas de corresponsalía extranjeras” en la página 68 y la sección de visión general ampliada “Cuentas de corresponsalía (extranjeras)” en la página 98.

Visión general fundamental – Informes sobre bancos extranjeros y cuentas financieras

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios de los informes sobre bancos extranjeros y cuentas financieras.

VISIÓN GENERAL

Toda persona[87] (incluyendo a los bancos) sujeta a la jurisdicción de EE. UU. que tenga participación financiera o autoridad para firmar en un banco, cuenta de títulos valores o cualquier otra cuenta financiera en un país extranjero, debe radicar el [formulario de] Informe de bancos extranjeros y cuentas financieras (FBAR [Report of a Foreign Bank and Financial Accounts]) ante el Servicio de Ingresos Nacionales (IRS) (TD F 90-22.1) si el

valor agregado de esas cuentas financieras supera los US $10.000 en cualquier momento del año calendario. Los bancos deben radicar este formulario sobre sus propias cuentas que cumplan con esta definición. Es posible que deban radicarlo con respecto a las cuentas en que el banco tiene una participación financiera o en las cuales tiene autorización para firmar.

Para las cuentas financieras extranjeras que pasen de US $10.000 en cualquier momento durante el año calendario anterior, se deben radicar los FBAR ante el comisionado del IRS [órgano tributario de EE. UU.] a más tardar el 30 de junio de cada año calendario.

Como se define en 31 CFR 103.11(z), el término "persona" significa un individuo, corporación, sociedad, fiducia o patrimonio de bienes [estate], sociedad anómina, asociación, consorcio de bancos [syndicate], asociación de riesgo compartido [joint venture] u otra organización o grupo sin personería jurídica [unincorporated], tribu indígena (como se define el término en la Ley de Regulación de Juegos en Comunidades Indígenas) [Indian Gaming Regulatory Act], y todas las entidades reconocidas como personas jurídicas.

Visión general fundamental – Informes sobre el transporte internacional de moneda o instrumentos financieros

OBJETIVO

Evaluar el cumplimiento del banco con los requerimientos estatutarios y regulatorios de los informes sobre el transporte internacional de moneda e instrumentos financieros.

VISIÓN GENERAL

Toda persona[88] (incluyendo a los bancos) que físicamente transporte o envíe por correo o de otra forma moneda o instrumentos financieros por un valor superior a los US $10.000

en un solo envío dirigido hacia el extranjero o hacia los Estados Unidos (y todo quien sea responsable de dicho transporte o envío por correo o de otra forma) debe radicar el Informe de transporte internacional de moneda o instrumentos financieros (CMIR) [International Transportation of Currency or Monetary Instruments]) (Formulario FinCEN 105). El CMIR se debe radicar ante un funcionario de la Oficina de Aduanas y Protección Fronteriza correspondiente o ante el Comisionado de aduanas en el momento de ingreso o salida de los Estados Unidos. Cuando una persona recibe moneda o instrumentos financieros por un monto superior a los US $10.000 en una sola ocasión, que han sido enviados desde cualquier lugar fuera de los Estados Unidos, se debe presentar un CMIR ante la Oficina de Aduanas adecuada o con el Comisionado de aduanas dentro de los quince (15) días siguientes al recibo de los instrumentos (salvo si ya se ha radicado un informe). El informe debe ser elaborado por quien solicita la transferencia de la moneda o los instrumentos monetarios o en nombre de la misma. Sin embargo, no es necesario que los bancos reporten estos aspectos si el envío se realiza por correo postal o por medio de portadoras [transportadoras] corrientes.[89] Además, los bancos comerciales o empresas fiduciarias organizadas bajo las leyes de cualquier estado o de los Estados Unidos no están obligadas a reportar los envíos de moneda o instrumentos monetarios efectuados por vía terrestre, si los remite o recibe un cliente establecido que tiene una relación de depósito con el banco y si el banco concluye razonablemente que los montos no exceden lo que corresponde a las prácticas acostumbradas del negocio, industria o profesión del cliente en cuestión.

La gerencia debe fijar políticas, procedimientos y trámites para la presentación del informe CMIR. La gerencia debe revisar el transporte internacional de moneda e instrumentos monetarios y determinar si la actividad de un cliente es usual y acostumbrada para el tipo de negocio en cuestión. Si no lo es, debe considerarse un Reporte de operaciones sospechosas.

[88] Id [*Nota del Traductor*: Ibid.]

En contraste, los bancos deben radicar el CMIR para reportar envíos de moneda o instrumentos monetarios a oficinas en el extranjero cuando esos envíos los realiza personal del banco directamente, como en el casos de envíos de moneda manejados por empleados del banco en los que se usan vehículos de propiedad del mismo banco.

MANUAL DE EXAMINADORES -LEY DEL SECRETO BANCARIO Y LUCHA CONTRA EL LAVADO DE DINERO

Visión general fundamental – Oficina de Control de Activos Extranjeros (OFAC)

OBJETIVO

Evaluar si el programa de la Oficina de Control de Activos Extranjeros (OFAC – Office of Foreign Assets Control) del banco, el cual debe estar basado en riesgo, es adecuado para el riesgo OFAC del banco, tomando en cuenta sus productos, servicios, clientes, transacciones y localizaciones geográficas.

ANTECEDENTES

La OFAC es una oficina adscrita al Tesoro de los Estados Unidos que administra y ejecuta sanciones económicas y comerciales basadas en la política exterior y las metas de seguridad nacional de los EE. UU., contra entidades tales como países extranjeros [que han sido declarados] objetivo, terroristas, narcotraficantes internacionales y quienes participan en actividades relacionadas con la proliferación de armas de destrucción masiva.

La OFAC actúa bajo facultades presidenciales especiales para situaciones de guerra y emergencia nacional otorgadas por legislación específica, con el objetivo de imponer controles a las transacciones y congelar activos bajo la jurisdicción de EE. UU. Muchas de las sanciones se basan en mandatos internacionales y de las Naciones Unidas y por lo tanto tienen un alcance multilateral, e implican cooperación estrecha con gobiernos aliados. Otras sanciones corresponden a intereses concretos de los Estados Unidos. El Secretario del Tesoro le ha delegado la responsabilidad a la OFAC de desarrollar, promulgar y administrar los programas de sanciones de los EE. UU.[90]

Todas las personas de EE. UU.,[91] incluyendo los bancos de EE. UU., sociedades que poseen o controlan bancos [bank holding companies] y sucursales no bancarias deben

Ley de Comercio con el Enemigo (TWEA), 50 USC App 1-4; Ley de Poderes de Emergencia Económica Internacional (IEEPA), 50 USC 1701 et seq.; Ley Antiterrorismo y Pena de Muerte Eficaz (AEDPA), 8 USC 1189, 18 USC 2339B; Ley de Participación de las Naciones Unidas 8 (UNPA), 22 USC 287c; Ley de Democracia Cubana (CDA), 22 USC 6001-10; Ley de Libertad y Solidaridad Democrática con Cuba (Ley de Libertad), 22 USC 6021-91; Ley de Comercio en Diamantes Limpios, Pub L. No. 108-19; Ley de Designación de Capos Internacionales del Narcotráfico (Ley de Capos) 21 USC 1901-1908,8 USC 1182; Ley de Libertad y Democracia de Burma de 2003, Pub. L. No. 108-61, 117 Stat. 864 (2003); Ley de Apropiaciones de las Operaciones Financieras, Financiación de las Exportaciones y Programas Relacionados, Sec. 570 de Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); Ley de Sanciones a Irak, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); Ley de Cooperación de Seguridad Internacional y Desarrollo, 22 USC 2349 aa8-9; Ley de Reforma a las Sanciones Comerciales y Mejoramiento de la Exportación de 2000, Título IX, Pub. L, No. 106-387 (octubre 28 de 2000).

[91] Todas las personas de EE. UU. deben cumplir con las regulaciones de la OFAC, incluyendo a todos los ciudadanos de EE. UU. y extranjeros que son residentes permanentes, no importa dónde estén ubicados, [y] todas las personas y entidades que están en los Estados Unidos, todas las entidades constituidas en los

cumplir con las regulaciones de la OFAC.[92] Las agencias bancarias federales evalúan los sistemas de cumplimiento para asegurarse de que todos los bancos sujetos a su supervisión cumplan con las sanciones.[93] A diferencia de la Ley del Secreto Bancario, las leyes y regulaciones emitidas por la OFAC aplican no solo a los bancos de EE. UU., sus sucursales nacionales, agencias, e infraestructuras internacionales de operaciones bancarias, sino también a sus sucursales extranjeras, y con frecuencia a las oficinas y sucursales de ultramar. En general, las regulaciones requieren lo siguiente:

. • Bloquear cuentas y otras propiedades de países, entidades y personas especificadas.
. • Prohibir o rechazar el comercio sin licencia y las transacciones financieras

con los países, entidades y personas especificadas.

Transacciones bloqueadas

La ley de EE. UU. requiere bloquear activos y cuentas cuando dichas propiedades están ubicadas en Estados Unidos, están en manos de personas o entidades estadounidenses o llegan a ser de propiedad o a estar bajo el control de personas o entidades estadounidenses. Por ejemplo, si una transferencia de fondos viene desde un sitio extraterritorial y está siendo encausada a través de un banco de EE. UU. a un banco extraterritorial, y la OFAC ha designado a alguien a dicha la transacción, la transacción se debe bloquear. La definición de activos y propiedad es amplia y se define específicamente en cada programa de sanción. Los activos y la propiedad incluyen cualquier cosa de valor directo, indirecto, presente, futuro o contingente (incluyendo todo tipo de transacciones bancarias). Los bancos deben bloquear las transacciones que presenten las siguientes características:

- han sido efectuadas por una persona o entidad bloqueada o en su nombre;
- se realizan para una entidad bloqueada o a través de la misma; o
- están vinculadas a una transacción en la cual tiene intereses una persona o entidad bloqueada.

Por ejemplo, si un banco de EE. UU. recibe instrucciones de hacer un pago por transferencia de fondos que corresponde a una de estas categorías, debe realizar la orden de pago y colocar los fondos en una cuenta bloqueada.[94] No es posible cancelar o enmendar las órdenes de pago una vez recibidas por bancos de EE. UU. sin una autorización de la OFAC.

EE.UU. y sus sucursales extranjeras. En el caso de ciertos programas, tales como los que están dirigidos a Cuba y Corea del Norte, las sucursales extranjeras de propiedad de empresas de EE. UU. o que están controladas por éstas también deben cumplir. Ciertos programas también obligan a cumplir a las personas extranjeras que posean artículos de origen estadounidense.

Se encuentra información adicional en “Regulaciones de Control de activos erxtranjeros para la comunidad financiera”, disponible en el sitio web de la OFAC en www.treas.gov/ofac/.

[93] 31 CFR capítulo V.

[94] Una cuenta bloqueada es una cuenta segregada que gana intereses (a una tasa comercial razonable), la cual tiene a su nombre la propiedad del cliente hasta que el objetivo es sacado de la lista, el programa de sanciones es anulado, o el cliente obtiene una licencia de la OFAC autorizando la liberación de la propiedad.
En algunos casos se puede prohibir una transacción subyacente, pero no hay ningún interés bloqueable en la transacción (por ejemplo, la transacción no se debe aceptar, pero la OFAC no requiere bloquear los activos). En estos casos la transacción simplemente se rechaza, esto es, no se procesa. Por ejemplo, las Regulaciones de sanciones a Sudán prohíben transacciones que apoyen las actividades comerciales de Sudán. Por tanto los bancos de EE. UU. tendrían que rechazar las transferencias de fondos entre dos empresas que no son Personas nacionales o bloqueadas especialmente designadas (SDN por sus siglas en inglés) que efectúan una exportación a una empresa en Sudán que tampoco es una SDN. Puesto que las Sanciones de Sudán solo requieren bloquear transacciones con el Gobierno de

Sudán o las SDN, no habría intereses "bloqueables" en los fondos entre las dos empresas. No obstante, puesto que las transacciones constituirían un apoyo a la actividad comercial de Sudán, lo cual está prohibido, los bancos de EE. UU. no pueden procesar la transacción y simplemente la rechazan.

Es importante anotar que el esquema de la OFAC que establece prohibiciones contra ciertos países, entidades y personas es diferente y aparte de la regulación (31 CFR 103.121) que contiene el Programa de identificación del cliente (CIP – Customer Identification Program) de la Ley del Secreto Bancario, que exige a los bancos comparar las cuentas nuevas con las listas del gobierno en las que se consignan los nombres de quienes se sospecha o se sabe que son terroristas u organizaciones terroristas, dentro de un período razonable después de la apertura de la cuenta. Las listas de la OFAC no han sido designadas como listas del gobierno para los propósitos de la regla del CIP. Para orientarse mejor, se debe consultar la sección de la visión general fundamental titulada "Programa de identificación del cliente" en la página 30. Sin embargo, los requerimientos de la OFAC se derivan de otros estatutos que no están limitados al terrorismo, y las sanciones de la OFAC aplican a las transacciones, además de las relaciones de cuenta.

Licencias de la OFAC

Por medio de un proceso de expedición de licencias, la OFAC está facultada para permitir ciertas transacciones que están otrora prohibidas bajo sus regulaciones. La OFAC puede emitir una licencia para practicar una transacción que normalmente es prohibida, cuando concluye que la transacción no debilita los objetivos de las políticas de EE. UU. de determinado programa de sanciones, o que de otra forma se justifica debido a objetivos de seguridad nacional o política exterior de los Estados Unidos. La OFAC también puede promulgar licencias generales, con las cuales autoriza ciertas categorías de transacciones, tales como permitir cargos razonables de servicios en las cuentas bloqueadas, sin necesidad de una autorización individual en cada caso de parte de la OFAC. Estas licencias pueden encontrarse en las regulaciones de cada programa de sanciones (31 CFR, Capítulo V [Regulaciones]) y se puede acceder a ellas en el sitio web de la OFAC. Antes de tramitar las transacciones que pueden estar cubiertas por una licencia general, los bancos deben verificar que dichas transacciones cumplen con los criterios relevantes de la licencia general.[95]

La información sobre la licencia se encuentra en el sitio web de la OFAC: www.treas.gov/ofac o comunicándose con el departamento de Licencias de la OFAC en el teléfono 202-622-2480.

Las licencias específicas se emiten para cada caso y requieren una solicitud dirigida a: *Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, D.C. 20220*. La licencia es un documento emitido por la OFAC en el que se autoriza una transacción o conjunto de transacciones específicas. Para recibir una licencia específica, la persona o entidad que desea hacer la transacción debe enviar una solicitud a la OFAC. Si la transacción se compagina con algún programa de la política exterior de EE. UU., se expide la licencia. Si el cliente de un banco afirma poseer una licencia específica, el banco debe verificar que la transacción cumple con los términos de la licencia y debe obtener y guardar una copia de la licencia de autorización.

Informes de la OFAC

Los bancos deben reportar todos los bloqueos a la OFAC dentro de los diez (10) días siguientes al bloqueo, y cada año a más tardar el 30 de septiembre deben informar sobre los casos de bloqueo de activos (al 30 junio).[96] Una vez bloqueados los activos o los fondos, se deben colocar en una cuenta bloqueada. Las transacciones prohibidas que hayan sido bloqueadas también deben reportarse a la OFAC máximo a los diez (10) días de haber ocurrido.

Los bancos deben guardar registros completos y precisos de cada transacción bloqueada o rechazada durante un mínimo de cinco (5) años después de la fecha de la transacción. Se deben llevar registros de las propiedades bloqueadas durante el período que permanezcan bloqueadas y durante los cinco (5) años siguientes a la fecha en que la propiedad es desbloqueada.

En el sitio web de la OFAC puede encontrarse información adicional sobre las regulaciones de la OFAC, como el Programa de Sanciones y los panfletos sobre los Resúmenes de país; la lista SDN, tanto de personas como de entidades; acciones recientes de la OFAC; y el folleto sobre Preguntas frecuentes.[97]

PROGRAMA DE LA OFAC

Aunque no lo requiere ninguna regulación específica, sino más bien como práctica de operaciones bancarias sólidas y para asegurar el cumplimiento, los bancos deben establecer y mantener un programa OFAC escrito eficaz que sea adecuado a su perfil de riesgo OFAC (basado en productos, servicios, clientes y localización geográfica). El programa debe identificar las áreas de alto riesgo, proporcionar controles internos adecuados para realizar una detección sistemática e informar, establecer pruebas independientes para evaluar el cumplimiento, designar un empleado del banco o varios empleados como los responsables de evaluar el cumplimiento de la OFAC, y diseñar programas de capacitación de personal adecuado en todas las áreas pertinentes del banco. El programa OFAC de un banco debe corresponder al respectivo perfil de riesgo OFAC del mismo.

[96] El informe anual debe presentarse en el formulario TD F 90-22.50.

[97] La información se encuentra disponible en el sitio web de la OFAC: www.treas.gov/ofac o llamando al teléfono de urgencias de la OFAC: 800-540-6322.

 Un elemento fundamental de un programa OFAC sólido es la evaluación del banco de sus propias líneas de productos, base

de clientes, naturaleza de las transacciones e identificación de áreas de alto riesgo para las transacciones OFAC. La identificación inicial de clientes de alto riesgo para los fines de la OFAC puede hacerse como parte de los procedimientos CIP [Programa de identificación del cliente] y CDD [Debida diligencia del cliente] del banco. Puesto que las sanciones de la OFAC pueden alcanzar virtualmente todas las áreas de sus operaciones, los bancos deben considerar todo tipo de operaciones, productos y servicios cuando realicen su evaluación de riesgo y establezcan políticas, procedimientos y trámites adecuados. Una evaluación de riesgo eficaz debe estar compuesta por múltiples factores (como se describe con más detalle a continuación), y dependiendo de las circunstancias, ciertos factores pueden pesar más que otros.

Otro elemento a tomar en cuenta en la evaluación del riesgo son las partes de las cuentas y las transacciones. Las nuevas cuentas deben ser confrontadas con las listas de la OFAC antes de su apertura o al poco tiempo de ésta. No obstante, el grado hasta donde un banco podrá incluir a las partes de las cuentas si son distintas a los tenedores de las mismas (por ejemplo, beneficiarios, garantes, mandantes, titulares, tenedores nominativos de acciones, directores, signatarios y poderes jurídicos) en la revisión inicial de la OFAC durante el proceso de apertura de cuentas, y durante las revisiones posteriores de bases de datos de cuentas existentes, dependerá del perfil de riesgo del banco y de la tecnología disponible.

Con base en el perfil de riesgo OFAC del banco en cada área y según la tecnología disponible, éste debe fijar políticas, procedimientos y trámites para revisar las transacciones y las partes que intervienen en la transacción (por ejemplo, banco emisor, beneficiario, endosatario o jurisdicción). La OFAC ofrece orientación sobre las partes que participan en las transacciones de cheques. La guía dice que si un banco sabe o tiene razones para creer que una parte que participa en una transacción con cheque es objetivo de la OFAC y dicho banco procede a tramitar la transacción de todas formas, incurre en responsabilidad, especialmente con las transacciones manejadas personalmente en ubicaciones de alto riesgo. Por ejemplo, si un banco sabe o tiene razones para creer que en una transacción con cheque participa una parte o país prohibido por la OFAC, la OFAC esperaría una identificación oportuna y una acción apropiada.

En la evaluación del nivel de riesgo, los bancos deben hacer uso de su buen juicio y tomar en cuenta todos los indicadores de riesgo. Aunque la lista no es exhaustiva, algunos de los productos, servicios, clientes y localizaciones geográficas que pueden implicar un mayor nivel de riesgo para la OFAC son los siguientes:

. • Transferencias internacionales de fondos
. • Cuentas de extranjeros no residentes
. • Cuentas de clientes extranjeros
. • Cámara de compensación automática transfronteriza (ACH en inglés)
. • Cartas de crédito comerciales
. • Banca electrónica de transacciones
. • Cuentas de corresponsalía extranjeras
. • Cuentas para procesar pagos [payable through accounts]
. • Banca privada internacional
. • Oficinas y sucursales en el extranjero

El Apéndice M ("Matriz de cantidad de riesgo – Procedimientos OFAC") proporciona una guía a los examinadores para evaluar los riesgos OFAC que enfrentan los bancos. La evaluación del riesgo puede usarse para ayudar al examinador a establecer el alcance del examen de la OFAC. La información adicional sobre el riesgo de cumplimiento está consignada por la OFAC en su sitio web bajo el título "Preguntas más frecuentes" (http://www.treas.gov/offices/enforcement/ofac/faq/#finance).

Una vez el banco ha identificado estas áreas de alto riesgo OFAC, debe fijar políticas, procedimientos y trámites adecuados para enfrentar los riesgos asociados. Los bancos pueden ajustar estas políticas, procedimientos y trámites a la naturaleza específica de una línea de negocios o producto. Además, se incentiva a los bancos para que evalúen periódicamente sus riesgos OFAC.

Controles internos

Un programa OFAC eficaz debe tener controles internos para identificar las cuentas y transacciones sospechosas e informar a la OFAC. Los controles internos deben incluir los siguientes elementos:

Marcación y revisión de transacciones sospechosas

Las políticas, procedimientos y trámites deben definir la manera en que el banco habrá de marcar y revisar transacciones y cuentas para detectar posibles violaciones OFAC, ya sea manualmente, a través de un software de interdicción, o mediante una combinación de ambos. Para los fines de filtración, los bancos deben definir claramente los criterios que emplearán al comparar los nombres de las listas suministradas por la OFAC con los nombres consignados en los archivos del banco o en las transacciones, así como al marcar transacciones o cuentas de países sancionados. Las políticas, procedimientos y trámites de los bancos también deben establecer cómo se procederá a determinar si un acierto inicial [con respecto a las listas] de la OFAC es una correspondencia válida o un falso positivo.[98] Un alto volumen de falsos positivos puede indicar la necesidad de revisar el programa de interdicción del banco.

Los criterios de filtración empleados por los bancos para identificar variaciones en los nombres y errores de ortografía deben basarse en el nivel de riesgo OFAC del producto o tipo de transacción particular. Por ejemplo, en un área de alto riesgo con alto volumen de transacciones, el software de interdicción debe permitir marcar las derivaciones cercanas de los nombres para su revisión. La lista SDN procura proporcionar derivaciones de nombres; sin embargo, es posible que no incluya todas las derivaciones posibles. Un software de interdicción más sofisticado puede captar las variaciones de un nombre SDN que no está incluido en la lista SDN. Los bancos o áreas de bajo riesgo y aquellos que tienen volumen bajo de transacciones, pueden optar por filtrar manualmente el cumplimiento con la OFAC. La decisión de usar software de

[98] Los pasos de la debida diligencia para establecer una asignación válida se proporcionan en "Cómo usar la línea caliente [línea de urgencias] de la OFAC" que se encuentra en el sitio web de la OFAC:

www.treas.gov/ofac.
interdicción y el nivel de sensibilidad del mismo deben basarse en la evaluación del banco de su propio riesgo y del volumen de sus transacciones. Para determinar la frecuencia de las verificaciones de la OFAC y los criterios de filtro usados (por ejemplo, derivaciones de nombres) los bancos deben tomar en cuenta la probabilidad de incurrir en una violación, así como la tecnología disponible. Además, los bancos deben reevaluar periódicamente su sistema de filtro OFAC. Por ejemplo, si un banco identifica una derivación de un nombre que es un objetivo de la OFAC, ésta sugiere que el banco agregue el nombre a su proceso de filtrado.

Las cuentas nuevas deben comparase con las listas de la OFAC antes de abrirse o poco tiempo después de abiertas (por ejemplo, durante el procesamiento nocturno). Los bancos que realizan las verificaciones OFAC después de la apertura de cuenta deben contar con procedimientos dirigidos a evitar transacciones, diferentes al depósito inicial, hasta que se haya completado la verificación OFAC. La realización de transacciones prohibidas antes de que se realice la verificación OFAC puede acarrear sanciones. Además, los bancos deben fijar políticas, procedimientos y trámites para examinar a los clientes actuales cuando se realizan adiciones o cambios en la lista de la OFAC. La frecuencia de la revisión debe basarse en el riesgo OFAC del banco. Por ejemplo, los bancos con un bajo nivel de riesgo OFAC deben comparar periódicamente (por ejemplo, mensualmente o trimestralmente) la base de clientes con la lista de la OFAC. Transacciones tales como transferencias de fondos, cartas de crédito y transacciones realizadas por personas no clientes, deben verificarse con la lista de la OFAC antes de ser ejecutadas. Al establecer sus políticas, procedimientos y trámites OFAC, los bancos deben tener siempre en cuenta que la OFAC considera la operación continua de una cuenta o el procesamiento de transacciones después de una designación, así como la idoneidad de su programa de cumplimiento con la OFAC, como factores que cuentan en el momento de determinar sanciones. Los bancos deben documentar sus verificaciones OFAC de las cuentas nuevas, de la base de clientes y de transacciones específicas.

Si el banco utiliza a un tercero como agente o proveedor de servicios para realizar las verificaciones OFAC en su nombre, ocurre como con cualquier otra obligación realizada por terceros: el banco es quien tiene la responsabilidad última del cumplimiento del tercero con los requerimientos de la OFAC. Como resultado, los bancos deben establecer controles adecuados y revisar los procedimientos para tales relaciones.

Actualización de las listas de la OFAC

El programa OFAC de un banco debe incluir políticas, procedimientos y trámites para la actualización oportuna de las listas de países, entidades y personas bloqueadas y la divulgación de esta información a través de las operaciones nacionales del banco y sus oficinas extraterritoriales, sucursales y, en el caso de Cuba y Corea del Norte, subsidiarias extranjeras.

Informes

El programa OFAC debe incluir también políticas, procedimientos y trámites para manejar

elementos que han sido válidamente bloqueados y rechazados bajo los diferentes programas de sanciones. En el caso de las interdicciones relacionadas con el narcotráfico o el terrorismo, los bancos deben notificar a la OFAC lo más pronto posible, por teléfono o por la línea caliente electrónica [e-hotline], sobre posibles aciertos, y enseguida hacer seguimiento mediante un documento escrito enviado dentro de los diez (10) días siguientes. La mayoría de los demás elementos se deben reportar a través de los conductos normales, máximo a los diez (10) días de haberse presentado. Las políticas, procedimientos y procesos también deben abordar el manejo de las cuentas bloqueadas. Los bancos tienen la responsabilidad de rastrear el monto de los fondos bloqueados, la propiedad de esos fondos, y los intereses pagados por concepto de los mismos. El monto total bloqueado, incluyendo intereses, debe reportarse a la OFAC a más tardar el 30 de septiembre de cada año (cubre información hasta el 30 de junio). Cuando un banco adquiere otro banco o se fusiona con él, ambos deben tomar en cuenta la necesidad de revisar y mantener dichos registros e información.

Los bancos ya no tienen que presentar los Informes de operaciones sospechosas (ROS) sobre transacciones bloqueadas relacionadas con el narcotráfico y el terrorismo, siempre que presenten a la OFAC el respectivo informe de bloqueo. No obstante, puesto que los informes de bloqueo requieren solo información limitada, si el banco posee información adicional que no aparece en el informe de bloqueo presentado a la OFAC, se debe radicar por aparte un reporte de operaciones sospechosas con FinCEN que incluya esa información. Además, el banco debe presentar un ROS si la misma transacción se consideraría sospechosa si no hay correspondencia válida con la información de la OFAC.[99]

Mantenimiento de la información de licencia

La OFAC recomienda que los bancos contemplen la posibilidad de mantener copias de las licencias OFAC de los clientes en sus archivos. Esto le permitiría a los bancos verificar si la transacción que inicia un cliente es legal. Los bancos deben también conocer la fecha de expiración de las licencias. Si no es claro si una transacción específica está autorizada por una licencia, el banco debe confirmar esto con la OFAC. Mantener copias de las licencias también es útil si otro banco en la cadena de pagos solicita verificar la validez de la licencia. Se deben mantener copias de las licencias durante los cinco (5) años siguientes a la última transacción realizada de conformidad con la licencia.

Pruebas independientes

Cada banco debe realizar una prueba independiente de su programa OFAC, efectuada por el departamento de auditoria interna, auditores externos, asesores u otros terceros calificados. En términos generales se debe efectuar una auditoria a profundidad por lo menos una vez al año. Para los bancos grandes, la frecuencia y el área de la prueba independiente se deben basar en el riesgo conocido o percibido de las áreas específicas del negocio. Para los bancos más pequeños, la auditoria debe ser consistente con el perfil de riesgo OFAC del banco, o basarse en el riesgo percibido. Las personas responsables de la prueba deben realizar una evaluación objetiva e integral de las políticas, procedimientos y trámites OFAC. El alcance

de la auditoria debe ser lo suficientemente integral para evaluar los riesgos de cumplimiento de la OFAC y evaluar qué tan adecuado es el programa de la OFAC.

[99] Ver el Comunicado de FinCEN Número 2004-02 "Presentación unitaria de Reportes de operaciones sospechosas y bloqueo" (69 *Registro Federal* 76847 de diciembre 23 de 2004).

Se recomienda que cada banco designe una(s) persona(s) calificada(s) como responsable(s) del cumplimiento diario del programa de la OFAC, incluyendo el informe de las transacciones bloqueadas o rechazadas de la OFAC, y la supervisión de los fondos bloqueados. La persona debe tener un nivel adecuado de conocimiento de las Regulaciones de la OFAC según el perfil de riesgo OFAC del banco.

Capacitación

El banco debe proporcionar capacitación adecuada a todos los empleados apropiados. El alcance y la frecuencia de la capacitación deben ser consistentes con el perfil de riesgo OFAC del banco y adecuadas para las responsabilidades del empleado.

Visión general fundamental – Conclusiones y finalización del examen

OBJETIVO

Formular conclusiones, comunicar los resultados a la gerencia, preparar comentarios a los informes, desarrollar una respuesta adecuada de parte de la supervisión y finalizar el examen.

VISIÓN GENERAL

En la fase final del examen de la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML), el examinador debe reunir todos los resultados de los procedimientos realizados. A partir de estos resultados el examinador debe sacar conclusiones sobre la idoneidad del programa de cumplimiento BSA/AML, analizar las conclusiones preliminares con la gerencia del banco, presentar estas conclusiones por escrito para incluirlas en el informe del examen, y determinar la respuesta regulatoria apropiada, si aplica.

Visión general ampliada – Programa de cumplimiento BSA/AML empresarial integral

OBJETIVO

Evaluar los programas de cumplimiento BSA/AML de las sociedades *holding* o de control o de las entidades financieras principales.[100]

VISIÓN GENERAL

Al igual que en el enfoque sobre el riesgo del crédito consolidado, riesgo del mercado y riesgo operacional, el control eficaz del riesgo BSA/AML puede requerir una gestión coordinada de riesgo. El programa de cumplimiento BSA/AML empresarial integral coordina los requerimientos regulatorios específicos a través de una organización en un marco de gestión de riesgo más amplio. Estos marcos le permiten a las organizaciones consolidar el conocimiento de su exposición al riesgo de lavado de dinero y financiación del terrorismo en todas las unidades de negocios, funciones y personas jurídicas. Por ejemplo, la empresa *holding* o la entidad financiera principal deben contar con una función centralizada para evaluar el riesgo BSA/AML y la exposición mundial a un cliente dado, particularmente aquellos considerados de alto riesgo o sospechosos, conforme a las leyes aplicables.[101]

Muchas organizaciones, especialmente las más complejas con operaciones internacionales, implementan programas de cumplimiento BSA/AML empresariales integrales que realizan gestión de riesgo integral en todas las subsidiarias, líneas de negocios y tipos de riesgo (por ejemplo, reputación, cumplimiento o transacción). Algunas de las organizaciones bancarias más complejas y grandes procuran manejar sus riesgos creando enfoques integrales para toda la empresa para sus programas de cumplimiento BSA/AML. Estos programas administran el riesgo tanto a nivel operacional como estratégico.

Aunque actualmente la regulación no requiere que las empresas *holding* o entidades financieras principales adopten un programa de cumplimiento BSA/AML empresarial integral, muchas organizaciones ven esto como una herramienta fundamental para administrar los riesgos BSA/AML asociados a la falta de cumplimiento de las leyes y regulaciones BSA. Una práctica sólida para las organizaciones complejas consistiría en establecer programas eficaces en las empresas *holding* o entidades financieras principales que contemplen los riesgos BSA/AML en todas las personas jurídicas y le

La entidad financiera principal es la entidad financiera más grande, en términos de activos, en la estructura de la empresa *holding* [empresa propietaria o empresa que detenta el control], salvo si es designada de otra forma por la empresa *holding*.

[101] Para encontrar pautas adicionales consulte la sección de visión general ampliada titulada “Sucursales y oficinas extranjeras de bancos de EE. UU.”, página 107, la Guía del Comité de Supervisión Bancaria de Basilea en “Administración de riesgo del programa Conozca a su cliente” (KYC por sus siglas en inglés para ‘Know Your Customer’)”.

permitan a los gerentes demostrarle a sus juntas directivas que tienen programas de cumplimiento eficaces en la organización consolidada. Los programas deben reflejar la estructura de las organizaciones y ajustarse a su tamaño, complejidad y requerimientos jurídicos, los cuales pueden variar según la línea específica de negocios o la jurisdicción sede.[102]

El programa empresarial integral debe incluir un punto central donde se agregan los riesgos BSA/AML de toda la organización. Estructuralmente, la función se puede establecer a nivel

de la empresa *holding* o de la entidad financiera principal. Así, las organizaciones bancarias que implementan estos programas evalúan el riesgo en forma consolidada en todas las actividades, líneas de negocios y personas jurídicas. Esta consolidación puede darse a nivel nacional o incluso internacional, dependiendo de la localización de las operaciones. Los sistemas empresariales integrales que operan a nivel mundial deben tomar en cuenta las distintas jurisdicciones en las que operan, así como las leyes y requerimientos AML [Lucha contra el Lavado de Dinero] a los que están sujetos, e incorporarlos en sus programas generales. La auditoria interna debe evaluar el nivel de cumplimiento con el programa de cumplimiento empresarial BSA/AML.

SUCURSALES, AFILIADAS Y LÍNEAS DE NEGOCIOS

Una empresa *holding* o de control o una institución financiera principal pueden optar por implementar un programa de cumplimiento BSA/AML empresarial integral, ya sea para toda la empresa o para funciones de negocios específicas (por ejemplo, sistemas de auditoria o de monitoreo de actividades sospechosas). Cuando se manejan así las funciones específicas de negocios, en un examen [o inspección] los examinadores deben identificar qué parte del programa de cumplimiento BSA/AML hace parte del programa empresarial integral. Esta información es fundamental para el diseño del alcance y la planeación del examen BSA/AML.

Al evaluar el programa de cumplimiento empresarial integral BSA/AML para determinar si es idóneo, el examinador debe establecer lineamientos para los informes y determinar cómo se ajusta cada sucursal en la estructura general de cumplimiento empresarial integral. El examinador debe evaluar cuán eficazmente la empresa *holding*
o la entidad financiera principal monitorean el cumplimiento en toda la organización mediante el programa de cumplimiento BSA/AML empresarial integral, incluyendo qué tan bien capta el sistema empresarial integral los datos relevantes de las sucursales.

La evaluación del programa de cumplimiento BSA/AML empresarial integral debe reflejar la evaluación de la idoneidad de los programas individuales de cumplimiento BSA/AML de las sucursales. Independientemente de la decisión de implementar un programa de cumplimiento BSA/AML empresarial integral entero o parcial, el programa debe asegurar que todos los afiliados cumplan con los requerimientos regulatorios aplicables. Por ejemplo, un programa de auditoria implementado exclusivamente a nivel de toda la empresa que no lleva a cabo pruebas de transacciones en todas las filiales del banco, no lograría cumplir con los requerimientos regulatorios de pruebas independientes para esas filiales bancarias.

Las políticas y procedimientos a nivel de sucursales y oficinas deben ser consistentes con los estándares del grupo o la empresa *holding*, aunque no tienen que ser necesariamente idénticos.

Las compañías *holding* o de control que administran centralmente las operaciones y funciones de sus sucursales bancarias y otras sucursales, deben tener políticas, procedimientos y procesos integrales de gestión de riesgo para cubrir toda la gama de riesgos. Un programa adecuado de cumplimiento BSA/AML empresarial integral de una

empresa *holding* proporcionaría el marco para que todas las sucursales y oficinas extranjeras cumplan con sus requerimientos regulatorios específicos (por ejemplo, del país o de la industria). De la misma manera, las organizaciones que administran centralmente programas de cumplimiento BSA/AML empresariales integrales, deben proporcionar una estructura adecuada, diseñar pautas y fijar límites de riesgo consistentes con sus actividades nacionales e internacionales. Para conocer más pautas, consulte la sección de visión ampliada titulada "Sucursales y oficinas extranjeras de bancos de EE. UU." en la página 107.

Las organizaciones que implementan programas de cumplimiento BSA/AML empresariales integrales deben evaluar el riesgo consolidado en todas las actividades, líneas de negocios y entidades. Con frecuencia las organizaciones usan software o soluciones de programación como ayudas en la implementación del programa de cumplimiento BSA/AML; estas soluciones típicamente incluyen, sin limitarse únicamente a ello, monitoreo, identificación y reportes de operaciones sospechosas. Algunas empresas *holding* estructuran sus programas empresariales integrales con el objetivo de administrar en forma centralizada únicamente ciertas funciones específicas del programa de cumplimiento BSA/AML (por ejemplo, la información de gestión de riesgo de los clientes de alto riesgo, cierres de cuentas, auditorias y sistemas de monitoreo de actividades sospechosas).

Las empresas *holding* de bancos [empresas que poseen o controlan bancos] (BHC por las siglas en inglés, para bank holding company) o las sucursales no bancarias de las mismas, o las entidades financieras extranjeras sujetas a la Ley BHC [Ley de sociedades que poseen o controlan bancos] o sucursales no bancarias de dichas entidades financieras extranjeras que operan en los Estados Unidos, están obligadas a radicar el Informe de operaciones sospechosas (ROS) con las agencias federales apropiadas de control, la Reserva Federal y el Tesoro de los EE. UU., según lo establece el literal 12 CFR 225.4(f). Ciertas empresas *holding* de corporaciones de ahorros y vivienda [savings and loan companies] y sus sucursales no depositarias, están obligadas a presentar el ROS según las regulaciones del Tesoro. Además, se recomienda muy enfáticamente que las empresas propietarias de corporaciones de ahorros y vivienda, si bien no están obligadas a hacerlo, de todas formas presenten el ROS cuando las circunstancias lo ameriten.

Visión general ampliada – Cuentas de corresponsalía (nacionales)

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a la oferta de relaciones de cuentas de corresponsalía nacionales, y la capacidad de la gerencia para implementar sistemas eficaces de monitoreo e información.

VISIÓN GENERAL

Los bancos mantienen relaciones de corresponsalía en otros bancos para proporcionar ciertos servicios que pueden lograrse de forma más económica o eficaz debido al tamaño, la

experiencia en una línea de negocios específica o la ubicación geográfica del otro banco. Estos servicios pueden incluir lo siguiente:

. • 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 derivarse de la recolección de elementos en efectivo y cartas en efectivo, transferencia y liquidación de transacciones de títulos valores, transferencia de fondos de préstamos participantes, compra o venta de fondos federales o procesamiento de transacciones de los clientes.
. • Otros servicios: Los servicios incluyen procesamiento de participaciones de préstamos, facilitar ventas de préstamos al mercado secundario [secondary market loan sales], procesamiento de datos y servicios de nómina y cambio de moneda extranjera.

Bancos de los banqueros

Los bancos de banqueros se fundan y constituyen para negociar con otros bancos y por lo general son propiedad de los bancos a los que sirven. Los bancos de banqueros no negocian directamente con el público. Ofrecen servicios bancarios de corresponsalía a bancos comunitarios independientes, entidades de ahorro y crédito [thrifts], cooperativas de ahorro y préstamo [credit unions] y fiducias de inversión en finca raíz [real estate investment trusts]. Los bancos de los banqueros proporcionan servicios directamente o mediante contratación externa o al patrocinar o endosar a terceros. Los productos que ofrecen los bancos de los banqueros por lo general consisten en servicios tradicionales de bancos de corresponsalía.

FACTORES DE RIESGO

Debido a que los bancos nacionales deben seguir los mismos requerimientos regulatorios, los riesgos BSA/AML en los bancos de corresponsalía nacionales son mínimos en comparación con otros tipos de servicios financieros. No obstante, cada banco adopta su propio enfoque al desarrollar su programa de cumplimiento BSA/AML, lo mismo que para la debida diligencia del cliente, los sistemas de información de gestión, el monitoreo de cuentas y los reportes de operaciones sospechosas. Además, si bien es posible que las cuentas de corresponsalía nacionales no se consideren de alto riesgo, las transacciones realizadas a través de esas cuentas, que pueden ser efectuadas en nombre del cliente de banco representado [respondent bank], sí pueden implicar alto riesgo.

FORMAS DE MITIGAR EL RIESGO

Los bancos que ofrecen servicios bancarios de corresponsalía a otros bancos nacionales (estos últimos se conocen como bancos representados [respondent banks]) deben fijar políticas, procedimientos y procesos para administrar los riesgos BSA/AML que surgen en

estas relaciones de corresponsalía y para detectar y reportar operaciones sospechosas. El nivel de riesgo varía dependiendo del programa de cumplimiento BSA/AML del banco corresponsal y de sus productos, servicios, clientes y localización geográfica. Cada banco debe monitorear las transacciones relacionadas con las cuentas de corresponsalía nacionales.

Visión general ampliada – Cuentas de corresponsalía (extranjeras)

OBJETIVO

Evaluar si los sistemas de los bancos de EE. UU. son adecuados para manejar los riesgos asociados a las relaciones de corresponsalía extranjeras y la capacidad de la gerencia para implementar sistemas eficaces de debida diligencia, monitoreo y reportes. Esta sección amplía la revisión fundamental previa de los requerimientos estatutarios y regulatorios de las relaciones de cuenta de entidades financieras de corresponsalía extranjeras, para ofrecer una evaluación más amplia de los riesgos AML asociados a esta actividad.

VISIÓN GENERAL

Las entidades financieras extranjeras mantienen cuentas en los bancos de EE. UU. para acceder al sistema financiero de ese país y aprovechar servicios y productos que pueden no estar disponibles en la jurisdicción de la entidad financiera extranjera. Estos servicios se requieren porque los bancos de EE. UU. los pueden prestar de manera más económica y eficaz o por otras razones, como por ejemplo para facilitar el comercio internacional. Los servicios pueden incluir lo siguiente:

. • Servicios de administración de efectivo, incluyendo cuentas de depósito
. • Transferencias internacionales de fondos
. • Canje de cheques
. • Cuentas para efectuar pagos [payable through accounts]
. • Actividades de transporte de valores bancarios [pouch activities]
. • Servicios de cambio de moneda extranjera
. • Cuenta de reinversión automática (cuentas de ‘barrido’) [sweep accounts]
. • Préstamos y cartas de crédito.

Acuerdos contractuales

Las relaciones de los bancos de EE. UU. con entidades financieras corresponsales deben regirse por acuerdos o contratos que especifiquen las obligaciones de cada una de las partes y otros detalles de la relación (por ejemplo, productos y servicios que se ofrecen, aceptación de depósitos, canje, formas de pago y tipos de endosos que se aceptan). El acuerdo o contrato debe también considerar las responsabilidades AML [Lucha contra el Lavado de Dinero] del corresponsal extranjero y su base de clientes, procedimientos de debida diligencia y la remisión de clientes desde el corresponsal hasta el banco de EE. UU., definiendo claramente todos los términos de la remisión (por ejemplo, tipo de cliente y

perfil de negocios, localización geográfica del cliente y términos especiales).

FACTORES DE RIESGO

Algunas entidades financieras extranjeras no están sujetas a las mismas pautas regulatorias que sí aplican para los bancos de EE. UU. y por lo tanto esas entidades pueden representar un riesgo de lavado de dinero mayor para el banco corresponsal en los EE. UU. Se han realizado investigaciones que demuestran que las cuentas de corresponsalía extranjeras han sido utilizadas por narcotraficantes y otros delincuentes para lavar fondos. A veces se usan empresas ficticias o de fachada en el proceso de distribución [layering process] para ocultar la verdadera propiedad de las cuentas en las entidades financieras corresponsales extranjeras. Debido al gran número de fondos, a las múltiples transacciones y la posible falta de familiaridad de los bancos de EE. UU. con los clientes de las entidades 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 de EE. UU. debe vigilar cuidadosamente las transacciones relacionadas con las cuentas de corresponsalía extranjeras.

Sin los controles adecuados, los bancos de EE. UU. también pueden abrir cuentas de corresponsalía tradicionales con entidades financieras extranjeras sin saber que la entidad financiera extranjera le permite a algunos clientes realizar transacciones en forma anónima a través de la cuenta en el banco de EE. UU. (por ejemplo, cuentas para realizar pagos[103] y cuentas anidadas [nested accounts]).

Cuentas "anidadas" [Nested Accounts]

Las cuentas 'anidadas' se producen cuando una entidad financiera extranjera logra acceder al sistema financiero de los EE. UU. a través de una cuenta de corresponsalía de EE. UU. que pertenece a otra entidad financiera extranjera. Si el banco de EE. UU. no sabe que su cliente de la entidad financiera corresponsal extranjera permite dicho acceso a terceras entidades financieras extranjeras, éstas pueden acceder efectivamente en forma anónima al sistema financiero de EE. UU. El comportamiento que indica la existencia de cuentas anidadas y otras cuentas de cuidado incluye transacciones dirigidas a jurisdicciones en las cuales la entidad financiera extranjera no tiene actividades de negocio conocidas ni intereses, y las transacciones cuyo volumen total supera significativamente la actividad previsible de la entidad financiera extranjera, según su base de clientes y el tamaño de sus activos.

FORMAS DE MITIGAR EL RIESGO

Los bancos de EE. UU. que ofrecen los servicios de entidades financieras extranjeras corresponsales deben fijar políticas, procedimientos y procesos para administrar los riesgos BSA/AML inherentes a estas relaciones, y monitorear cuidadosamente las transacciones relacionadas con estas cuentas para detectar y reportar operaciones sospechosas. El nivel de

riesgo varía según los productos, servicios, clientes y localización geográfica de la entidad financiera extranjera. En la página 68 de la sección de visión general fundamental titulada "Registros de cuentas de corresponsalía extranjeras y debida diligencia" se puede encontrar información adicional sobre las evaluaciones de riesgo y la debida diligencia. Las políticas, procedimientos y procesos de los bancos de EE. UU. deben:

[103] Consulte la sección de la visión general ampliada titulada "Cuentas para pagos" ["Payable Through Accounts"] en la página 102 para conocer más información.

. • Conocer el propósito para el cual se quieren usar las cuentas y la actividad que se espera de las mismas (por ejemplo, determinar si la relación será utilizada como cuenta para pagos [desde el exterior]).

. • Conocer las demás relaciones de corresponsalía que pueda tener la entidad financiera extranjera (por ejemplo, determinar si se usarán cuentas anidadas).

. • Evaluar los riesgos que representan las relaciones de la entidad financiera corresponsal extranjera.

. • Realizar una adecuada debida diligencia permanente a las relaciones de la entidad financiera corresponsal extranjera, que puede incluir visitas periódicas.

. • Verificar que las relaciones de la entidad financiera corresponsal extranjera estén debidamente incluidas en los sistemas de monitoreo y reporte de operaciones sospechosas del banco de EE. UU.

. • Fijar criterios para cerrar las cuentas de las entidades financieras corresponsales extranjeras.

Como una buena práctica, se sugiere que los bancos de EE. UU. comuniquen sus expectativas sobre la lucha contra el lavado de dinero [AML] a los clientes de sus corresponsales financieras extranjeras. Además, los bancos de EE. UU. por lo general deben conocer los controles AML de las entidades financieras corresponsales extranjeras, incluyendo las prácticas de debida diligencia de la clientela y los registros de la documentación.

Visión general ampliada –Letras de cambio o libranzas en dólares de EE. UU. [US Dollar Drafts]

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a las letras o libranzas bancarias en dólares de EE. UU. y la capacidad de la gerencia para implementar sistemas eficaces de monitoreo y reporte.

VISIÓN GENERAL

Una letra de cambio en dólares de EE. UU. [US dollar draft] es una libranza o cheque bancario denominado en dólares de EE. UU. disponible en entidades financieras

extranjeras. Estos cheques los giran entidades financieras extranjeras sobre cuentas de corresponsalía en EE. UU. Con frecuencia los cheques se compran para pagar transacciones comerciales o personales y para cancelar obligaciones en el extranjero.

FACTORES DE RIESGO

La mayoría de los cheques en dólares de EE. UU. son legítimos; no obstante, se ha comprobado que son vulnerables al lavado de dinero. Las estratagemas en que se utilizan letras de cambio en dólares de EE. UU. pueden incluir el contrabando de moneda de EE. UU. hacia entidades financieras extranjeras para comprar cheques o letras de cambio denominadas en dólares estadounidenses. La entidad financiera extranjera acepta la moneda de EE. UU. y emite una libranza en dólares de EE. UU. girada contra su cuenta en el banco corresponsal de EE. UU. Una vez la moneda adopta la forma de letra bancaria, el lavador de dinero puede ocultar el origen de los fondos con más facilidad. La posibilidad de convertir ingresos ilícitos en letras bancarias en las entidades financieras extranjeras le facilita a los lavadores de dinero el transporte del instrumento, ya sea nuevamente hacia Estados Unidos, o su endoso a favor de terceros en jurisdicciones donde las leyes sobre el lavado de dinero, o el cumplimiento de las mismas, son laxas. De todas formas la persona logra lavar fondos ilícitos; y finalmente el giro o cheque es devuelto al banco corresponsal en EE. UU. para ser procesado.

FORMAS DE MITIGAR EL RIESGO

Las políticas, procedimientos y procesos de los bancos de EE. UU. deben incluir lo siguiente:

. • Describir los criterios que rigen la apertura de una relación de libranzas en dólares de EE. UU. con una institución o entidad financiera extranjera (por ejemplo, jurisdicción; productos, servicios, mercado objetivo; propósito de la cuenta y actividad prevista; o historial del cliente).
. • Detallar las transacciones que son y no son aceptables (por ejemplo, estructurar las transacciones o comprar múltiples giros numerados secuencialmente para un mismo beneficiario).
. • Detallar el monitoreo y reporte de operaciones sospechosas asociadas a las letras de cambio en dólares de EE. UU.
. • Discutir los criterios que determinan el cierre de las relaciones de cheques en dólares de EE. UU.

Visión general ampliada – Cuentas usadas para pagos [Payable Through Accounts]

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a las cuentas que se utilizan para efectuar pagos (PTA por sus siglas en inglés, para Payable

Through Accounts) y la capacidad de la gerencia de implementar sistemas eficaces de monitoreo y reporte.

VISIÓN GENERAL

Las instituciones financieras extranjeras usan las PTA, también conocidas como cuentas "de tránsito" o "de paso" para proporcionar a sus clientes acceso al sistema bancario de EE. UU. Algunos bancos de EE. UU., corporaciones de la Ley Edge [Edge Act] (corporaciones contratadas por la Reserva Federal para realizar operaciones bancarias internacionales) y corporaciones por contrato y sucursales y agencias de entidades financieras extranjeras (conocidas colectivamente como bancos de EE. UU.) ofrecen estas cuentas como un servicio a las entidades financieras extranjeras. Las autoridades judiciales han declarado que el riesgo de lavado de dinero y otras actividades ilícitas es alto en las cuentas PTA que no se controlan adecuadamente.

Generalmente una entidad financiera extranjera solicita una PTA para sus clientes que desean realizar transacciones en Estados Unidos a través de la cuenta de esa entidad financiera extranjera en un banco de EE. UU. La entidad financiera extranjera provee sus clientes, a los que se refiere comúnmente como "sub-cuenta habientes", con cheques que les permiten sacar fondos de la cuenta de esa entidad financiera extranjera en el banco de EE. UU.[104] Los sub-cuenta habientes, que pueden llegar a ser cientos o miles para una misma PTA, se convierten todos en signatarios en la cuenta de la entidad financiera extranjera en el banco de EE. UU. Si bien los clientes de estas cuentas de paso pueden girar cheques y hacer depósitos en el banco de Estados Unidos como cualquier otro cuenta habiente, generalmente no están directamente sujetos a los requisitos que rigen la apertura de cuentas en los bancos de Estados Unidos.

Las actividades PTA no se deben confundir con las relaciones tradicionales de operaciones bancarias de corresponsalía internacional, en las que una entidad financiera internacional celebra un contrato con banco de EE. UU. para procesar y tramitar transacciones a nombre de dicha entidad financiera internacional y sus clientes. Bajo este contrato de corresponsalía los clientes de la entidad financiera internacional no pueden acceder directamente a la cuenta corresponsal en el banco de EE. UU., pero si hacen transacciones a través de la cuenta en EE. UU. Este acuerdo se diferencia significativamente de las PTA con sub-cuenta habientes, porque éstos últimos sí pueden

[104] En este tipo de relación la entidad financiera extranjera se conoce como el "cuenta habiente maestro" ["master accountholder"].

FACTORES DE RIESGO

Las PTA tienden a presentar mayor riesgo porque los bancos de EE.UU. tradicionalmente no aplican los mismos requerimientos de debida diligencia a las PTA que sí aplican a los

clientes nacionales que desean abrir cuentas corrientes y otros tipos de cuenta. Por ejemplo, algunos bancos de EE.UU. tan sólo piden una copia de las tarjetas de firmas diligenciadas por los clientes de las cuentas de paso (que son los clientes de la entidad financiera extranjera). Entonces estos bancos de EE. UU. procesan miles de cheques de sub-cuenta habientes así como otras transacciones, incluyendo depósitos en moneda, a través de la PTA de la entidad financiera extranjera. En la mayoría de los casos se dedican pocos esfuerzos o ninguno a obtener o confirmar información sobre las personas o negocios de los sub-cuenta habientes que usan las PTA.

El empleo de las PTA por las entidades financieras extranjeras, conjuntamente con la inadecuada supervisión que ejercen los bancos de EE. UU., pueden facilitar prácticas bancarias poco confiables como el lavado de dinero y las actividades delictivas relacionadas. La posibilidad del lavado de dinero y la financiación del terrorismo, las violaciones a la OFAC y otros delitos graves aumenta si los bancos de EE. UU. no son capaces de identificar y conocer las transacciones de los usuarios finales (la mayoría de los cuales vive fuera de EE. UU.) de sus cuentas con corresponsales extranjeros. Las PTA utilizadas con fines ilícitos pueden generarle a los bancos graves pérdidas financieras representadas en multas penales y civiles, incautación y confiscación de garantías y daño a su reputación.

FORMAS DE MITIGAR EL RIESGO

Los bancos de EE. UU. que ofrecen servicios de PTA deben fijar y mantener políticas, procedimientos y procesos adecuados para tomar medidas contra el posible uso ilegal de las mismas. Como mínimo, las políticas, procedimientos y procesos deben permitirle a los bancos de EE.UU. identificar a los usuarios finales de las PTA de sus entidades financieras extranjeras e incluir la obtención (o la posibilidad lograrla a través de arreglos con terceros confiables) básicamente de la misma información sobre los usuarios finales de las PTA que se obtiene de los clientes directos.

Las políticas, procedimientos y trámites deben incluir una revisión de los procesos de identificación y monitoreo de las transacciones de los sub-cuenta habientes de la entidad financiera extranjera, y el cumplimiento de los requisitos estatutarios y regulatorios AML que tenga el país sede y el contrato principal de la entidad financiera extranjera con el banco de EE. UU. Además, los bancos de EE.UU. deben tener procedimientos para monitorear las transacciones realizadas a través de las PTA de las entidades financieras extranjeras.

Como parte de un esfuerzo dirigido a enfrentar el riesgo inherente de las PTA, los bancos de EE. UU. deben tener un contrato firmado (por ejemplo, contrato principal [master agreement]) que incluya lo siguiente:

- Funciones y responsabilidades de cada parte.
- Límites y restricciones sobre los tipos y montos de las transacciones (por ejemplo, depósitos en moneda, transferencias de fondos, cambio de cheques).
- Restricciones sobre los tipos de sub-cuenta habientes (por ejemplo, casas de cambio, empresas de financiación, remitentes de fondos y otras entidades financieras no

bancarias).

- Prohibiciones o restricciones sobre los sub-cuenta habientes multi-nivel.[105]
- Acceso a los documentos internos y auditorías de las entidades financieras extranjeras que hacen parte de las actividades de las PTA.

Los bancos de EE. UU. deben considerar la posibilidad de cerrar las PTA en las siguientes circunstancias:

- Información insuficiente sobre los usuarios finales de la PTA.
- Evidencia de operaciones sospechosas sustanciales o en curso.
- No poder demostrar que las PTA no están siendo utilizadas para lavar dinero u otros fines ilícitos.

[105] Es posible que una sub-cuenta se subdivida en varias sub-cuentas para personas individuales.

Manual de Exámenes – FFIEC BSA/AML 115
6/23/2005

Visión general ampliada – Actividades de transporte de valores bancarios (valija bancaria) [Pouch Activities]

OBJETIVO

Evaluar si los sistemas bancarios son adecuados para manejar los riesgos asociados a las actividades de transporte de valores bancarios [pouch activities] y las capacidad gerencial para implementar sistemas eficaces de monitoreo y reporte.

VISIÓN GENERAL

Las actividades de transporte implican la utilización de empresas de transporte, de servicios de correo rápido o *couriers* (independientes o corrientes) o de agentes de remisión empleados por los servicios de correo rápido o *couriers*,[106] para transportar moneda, instrumentos monetarios y otros documentos desde fuera de los Estados Unidos a bancos en los Estados Unidos.[107] Las valijas las pueden enviar otros bancos o personas. Los servicios de valija normalmente se ofrecen conjuntamente con servicios de banca corresponsal extranjera. Las valijas pueden tener pagos de préstamos, transacciones de cuentas de depósito de demanda y otros tipos de transacciones.

FACTORES DE RIESGO

Los bancos deben saber que con frecuencia se han encontrado en las valijas y en cartas de efectivo [cash letters] recibidas de entidades financieras extranjeras grandes números de instrumentos monetarios comprados en Estados Unidos que parecen haber sido

estructurados para evitar los requerimientos del informe BSA [Ley del Secreto Bancario]. Esto es especialmente válido en el caso de valijas y letras de efectivo recibidas de jurisdicciones cuyas estructuras AML [de Lucha contra el Lavado de Dinero] son laxas o deficientes. Los instrumentos monetarios involucrados con frecuencia son giros postales, cheques 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.
. • Están numerados consecutivamente y son por valores ligeramente inferiores a US $ 3.000 o $10.000.

Los agentes de remisión son personas o corporaciones extranjeras que están comprometidas contractualmente con el banco de EE. UU. Proporcionan servicios de representación a los clientes del banco en el extranjero a cambio de honorarios. Los servicios pueden ir desde la remisión de nuevos clientes al banco hasta la administración especial del correo, obtención y transporte de documentos, distribución de folletos y solicitudes o formularios del banco, escrituración o autenticación de documentos de los clientes y remisión por correo de los fondos de los clientes al banco en los Estados Unidos para consignarlos.

[107] Para una guía adicional, consulte la sección de la visión general fundamental titulada “Informes sobre el transporte internacional de moneda o instrumentos financieros” en la página 83.

. • Los espacios para 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 prontamente le sigue una transferencia de fondos hacia afuera por el mismo valor en dólares.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben fijar políticas, procedimientos y procesos relativos a las actividades de valija, los cuales deben:

- Describir los criterios de apertura de una relación de valija con una persona o entidad financiera extranjera (por ejemplo, requisitos de debida diligencia del cliente, 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, número elevado de instrumentos monetarios con numeración consecutiva).
. • Detallar los procedimientos para el procesamiento de la valija, incluyendo la responsabilidad de los empleados, dobles controles, requerimientos de conciliación y documentación, retiro de empleados.
. • Detallar los procedimientos de revisión de actividades inusuales o sospechosas, incluyendo escalar los casos a la gerencia (los contenidos de las valijas pueden estar sujetos a la obligación de presentar los siguientes informes: Informe de transacciones monetarias (CTR), Informe sobre transporte internacional de moneda o

instrumentos monetarios (CMIR), y Reporte de operaciones sospechosas (ROS)).

. • Discutir los criterios a emplear para el cierre de las relaciones de valija.

Los factores arriba mencionados deben incluirse en un acuerdo o contrato celebrado entre el banco y la empresa transportadora que detalle los servicios que se proporcionarán y las responsabilidades de las dos partes.

Visión general ampliada – Sucursales y oficinas extranjeras de bancos de EE. UU.

OBJETIVO

Evaluar si los sistemas de los bancos de EE. UU. son adecuados para manejar los riesgos asociados a sus sucursales y oficinas extranjeras, y la capacidad gerencial para implementar sistemas eficaces de monitoreo y reporte.

VISIÓN GENERAL

Los bancos de EE.UU. abren sucursales y oficinas[108] en el extranjero para satisfacer exigencias específicas de sus clientes, para que el banco crezca o para aumentar los productos o servicios que ofrecen. Las sucursales y oficinas extranjeras varían significativamente en cuanto a tamaño, complejidad de sus operaciones y alcance de los productos y servicios que ofrecen. Los examinadores deben tomar en cuenta estos factores al evaluar si las sucursales y oficinas extranjeras se adhieren al programa de cumplimiento de la Ley de Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML) del banco. Las políticas, procedimientos y procesos de Lucha contra el Lavado de Dinero (AML) de la oficina o sucursal extranjera deben cumplir con los requerimientos locales y ser consistentes con los estándares bancarios de los EE.UU; no obstante, es posible que requieran adaptación a las prácticas locales o comerciales.[109]

FACTORES DE RIESGO

Los examinadores deben conocer el tipo de productos y servicios que se ofrecen en las sucursales y oficinas extranjeras, así como los clientes y áreas geográficas que atienden. Todos los servicios que ofrecen los bancos de EE. UU. los pueden ofrecer las sucursales u oficinas extranjeras, salvo si están prohibidos en el país anfitrión. Esos productos y servicios pueden presentar un perfil de riesgo diferente al que tienen cuando los ofrecen bancos de EE. UU. (por ejemplo, los negocios de servicios de dinero [money services bussinesses] están vigilados en Estados Unidos, pero no necesariamente en otros países). Por tanto, el examinador debe saber que los riesgos que tienen las sucursales y oficinas extranjeras pueden variar (por ejemplo, operaciones mayoristas versus minoristas).

El examinador debe conocer los diferentes requerimientos de Lucha contra el Lavado de Dinero (AML) que tienen las jurisdicciones extranjeras. La legislación sobre el secreto

[bancario] o su equivalente pueden afectar la posibilidad de que las sucursales u oficinas extranjeras compartan información con la casa matriz del banco, o la posibilidad de que el examinador lleve a cabo su inspección en la misma sede de esas oficinas. Aunque los

[108] Esto incluye afiliados y sucursales.

Para consultar información adicional ver el documento del Comité de Basilea sobre supervisión bancaria en "Gestión de riesgo del programa Conozca a su cliente" (KYC por sus siglas en inglés)" de 2004 en www.bis.org/publ.

requerimientos específicos de la Ley del Secreto Bancario (BSA) no aplican a las sucursales y oficinas extranjeras, sí se espera que, en todas sus sucursales y oficinas, los bancos fijen políticas, procedimientos y procesos de protección contra los riesgos de lavado de dinero y financiación del terrorismo. En este sentido las sucursales y oficinas extranjeras deben guiarse por las políticas, procedimientos y procesos de la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero (BSA/AML) del [respectivo] banco de los Estados Unidos. Dichas sucursales y oficinas extranjeras deben cumplir con los requerimientos de la Oficina de Control de Activos Extranjeros (OFAC) y todas las leyes, normas y regulaciones locales de Lucha contra el Lavado de Dinero (AML).

FORMAS DE MITIGAR EL RIESGO

Las sucursales y oficinas de los bancos de EE.UU ubicadas en zonas de alto riesgo pueden ser vulnerables al lavado de dinero. Para tratar este problema, las políticas, procedimientos y procesos de las operaciones realizadas en el extranjero deben acoger las siguientes recomendaciones:

. • Las oficinas principales y las gerencias de operaciones extranjeras de los bancos de EE. UU. deben conocer la eficacia y calidad de la supervisión bancaria del país anfitrión y los requerimientos legales y mecanismos de control del mismo. La oficina principal del banco de EE. UU. debe conocer y comprender los problemas que puedan tener los supervisores del país anfitrión con respecto a la oficina o sucursal extranjera.

. • La oficina principal del banco de EE.UU debe conocer el perfil de riesgo de las sucursales u oficinas extranjeras (por ejemplo, productos, servicios, clientes y localizaciones geográficas).

. • La oficina principal del banco de EE.UU debe contar con suficiente información para poder monitorear periódicamente la actividad de sus sucursales y oficinas, incluyendo el nivel de cumplimiento de las mismas con las políticas, procedimientos y procesos de la oficina principal. Esto se puede lograr en parte a través de informes de sistemas de información de gestión [management information systems reports].

. • La casa matriz del banco de EE.UU debe crear un sistema para probar y verificar la integridad y eficacia de los controles internos en las sucursales u oficinas extranjeras mediante auditorias realizadas en el país. La alta gerencia y la casa matriz debe recibir y revisar copias de los informes de auditoria escritos en inglés así como de cualquier otro informe relativo a las evaluaciones sobre lavado de dinero (AML) y controles internos.

. • La casa matriz del banco de EE.UU debe establecer prácticas bien

fundamentadas para la información compartida con sucursales y oficinas, particularmente con respecto a las relaciones de cuentas de alto riesgo.

. • La casa matriz del banco de EE.UU debe estar en capacidad de proporcionar a los examinadores toda la información que se considere necesaria para evaluar el cumplimiento con las leyes bancarias de los EE.UU.

Las estructuras de cumplimiento y auditoria de las sucursales y oficinas ubicadas en el exterior pueden variar sustancialmente dependiendo del alcance de las operaciones (por ejemplo, ubicación geográfica) y el tipo de productos, servicios y clientes. Las sucursales y oficinas del exterior que tienen múltiples sedes en una región (por ejemplo, Europa, Asia y América del Sur) con frecuencia son supervisadas por el personal de cumplimiento y auditoria regional. Independientemente del tamaño o el alcance de las operaciones, se debe contar con suficiente personal de cumplimiento y auditoria y suficientes programas de auditoria para vigilar el riesgo de lavado de dinero (AML).

DISEÑO DEL ALCANCE DE LOS EXÁMENES AML (de la Lucha contra el Lavado de Dinero)

Los exámenes o inspecciones pueden realizarse en el país anfitrión o en los Estados Unidos. Los factores que se toman en cuenta para decidir si la inspección se debe hacer en la jurisdicción anfitriona o en los Estados Unidos son los siguientes:

. • El perfil de riesgo de la sucursal u oficina extranjera y si éste es estable o cambia en el caso de una reorganización, introducción de nuevos productos o servicios u otros factores, incluyendo el perfil de riesgo de la jurisdicción en sí.
. • La eficacia y calidad de la supervisión bancaria en el país anfitrión.
. • Existencia de un acuerdo para compartir información entre el país sede y el supervisor de EE. UU.
. • Historial de asuntos relativos a los exámenes [la inspección] o auditorias en la sucursal u oficina extranjera.
. • El tamaño y la complejidad de las operaciones de la sucursal u oficina extranjera.
. • Eficacia de los controles internos, incluyendo sistemas para administrar los riesgos AML (de Lucha contra el Lavado de Dinero) a nivel consolidado y auditoria interna.
. • Capacidad gerencial de la sucursal u oficina extranjera para proteger a la entidad contra el lavado de dinero o la financiación del terrorismo.
. • Disponibilidad de los registros (historial) de la sucursal u oficina extranjera en los Estados Unidos.

En algunas jurisdicciones, la ley de secreto financiero y otras leyes pueden impedir o restringir severamente que los examinadores de EE. UU. o el personal de la casa matriz en EE. UU. evalúen directamente las actividades o los registros (el historial) de los clientes. Si no es posible realizar una inspección eficaz en el terreno, los examinadores deben consultar con el personal de una agencia adecuada. En esos casos el personal de la agencia puede comunicarse con los supervisores extranjeros para hacer arreglos apropiados sobre la información compartida o los planes para la inspección. En situaciones de bajo riesgo en las

que se restringe la información, los examinadores pueden realizar inspecciones desde los EE. UU. (ver el análisis consignado abajo). En situaciones de alto riesgo cuando no se puede realizar una inspección adecuada (en el terreno o de otra forma), es posible que la agencia le solicite a la casa matriz adoptar medidas para solucionar la situación. Dichas medidas pueden incluir cerrar la oficina extranjera.

Inspecciones desde los Estados Unidos

Las inspecciones realizadas desde EE. UU. o las que se hacen fuera de la sede de la entidad examinada, por lo general requieren mayor confianza en el programa de Lucha contra el Lavado de Dinero en la sucursal u oficina extranjera, así como la posibilidad de acceder a un número suficiente de registros. Las inspecciones realizadas por fuera de las sedes deben incluir conversaciones con los altos directivos de la casa matriz y las oficinas extranjeras, las cuales son esenciales para conocer las operaciones de las mismas, así como sus riesgos y programas AML (de Lucha contra el Lavado de Dinero). Además, el examen de la sucursal u oficina extranjera debe incluir una revisión de la participación del banco estadounidense en la administración o el monitoreo de las operaciones de la sucursal extranjera, los sistemas internos de control (por ejemplo, políticas, procedimientos e informes de monitoreo), y donde estén disponibles, los resultados, auditorías y documentos de trabajo de las inspecciones llevadas a cabo por los supervisores del país sede. Como en todas las inspecciones de Ley de Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML), la amplitud y profundidad del análisis de transacciones y actividades, donde éste se realice, se basa en diferentes factores que incluyen el criterio del examinador sobre los riesgos, los controles y la idoneidad de las pruebas independientes.

Inspecciones basadas en la jurisdicción anfitriona

El proceso estándar de diseño del alcance y planeación determinará el enfoque del examen y los recursos requeridos. Puede haber algunas diferencias en el proceso de examen realizado en el exterior. El ente supervisor del país anfitrión puede enviar un supervisor para que trabaje conjuntamente con el equipo de los Estados Unidos, o solicitar autorización para asistir a las reuniones al inicio y en la conclusión de la inspección.

También es probable que los requisitos para la elaboración de los informes de Lucha contra el Lavado de Dinero sean diferentes, puesto que se ajustan a la regulación local. Además, el trabajo hecho sobre el terreno en la jurisdicción anfitriona le permite a los examinadores conocer mejor la función del banco de EE. UU. en relación con su sucursal u oficina extranjera.

Tanto para las inspecciones realizadas desde EE. UU. como para las realizadas en el país anfitrión, los procedimientos utilizados para productos, servicios y clientes específicos son que están consignados en este manual. Por ejemplo, si un examinador está examinando las actividades de valija [o transporte de moneda o instrumentos bancarios] (pouch activities) en las sucursales u oficinas extranjeras, debe usar los procedimientos de inspección ampliados que apliquen al caso.

Visión general ampliada – Banca paralela

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a las relaciones de banca paralela, y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Existe una organización de banca paralela cuando por lo menos un (1) banco estadounidense y una (1) entidad financiera extranjera son controlados directa o indirectamente por una misma persona o grupo de personas con estrecha relación comercial entre sí o que actúan en forma conjunta, sin estar sujetas a supervisión consolidada por un mismo supervisor del país anfitrión. La entidad financiera extranjera estará sujeta a distintas normas y controles de lavado de dinero y a una estructura de vigilancia y supervisión diferente, y éstas pueden ser menos rigurosas que las de los Estados Unidos. Las diferencias regulatorias y de supervisión incrementan los riesgos relativos a la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero (BSA/AML) que presentan las organizaciones de banca paralela.

FACTORES DE RIESGO

Las organizaciones de banca paralela pueden tener una administración común, compartir políticas y procedimientos, vender productos transversalmente, o estar por lo general vinculadas a una entidad financiera extranjera paralela en muchos sentidos. El principal problema de lavado de dinero que atañe a las organizaciones de banca paralela es que el banco estadounidense puede estar expuesto a mayor riesgo por las transacciones realizadas con la entidad financiera extranjera paralela. Las transacciones se pueden facilitar y los riesgos pueden aumentar debido a la ausencia de distanciamiento y procedimientos normales [lack of arm's length dealing] y por los controles reducidos que se aplican a las transacciones entre bancos que están vinculados o estrechamente asociados. Por ejemplo, es posible que compartan sus funcionarios o directores o que éstos trabajen conjuntamente aún si son diferentes.

FORMAS DE MITIGAR EL RIESGO

Las políticas, procedimientos y trámites de las relaciones de banca paralela deben ser compatibles con las de las demás relaciones de banca corresponsal extranjera. Además, los bancos paralelos deben:

. • Proporcionar líneas independientes de autoridad en la toma de decisiones.
. • Protegerse contra conflictos de intereses.

. • Emplear mecanismos de distanciamiento y salvaguardias normales en los negocios realizados entre las entidades relacionadas.

Visión general ampliada – Banca electrónica

OBJETIVO

Evaluar si los sistemas bancarios son adecuados para manejar los riesgos asociados a los clientes de banca electrónica (e-banking o transacciones bancarias a través de Internet) y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Los sistemas de transacciones bancarias electrónicas (e-banking), que proporcionan la entrega electrónica de productos bancarios a los clientes, incluyen las transacciones por cajero automático (ATM); apertura de cuentas por Internet; transacciones bancarias por Internet; y transacciones bancarias telefónicas. Por ejemplo, las tarjetas de crédito, las cuentas de depósito, préstamos hipotecarios y transferencia de fondos, pueden iniciarse a través del Internet, sin contacto cara a cara. Las gerencias deben reconocer que todo esto implica un potencial de alto riesgo y deben fijar políticas, procedimientos y procesos para identificar clientes y monitorear ciertas áreas concretas de las operaciones bancarias. Consulte la sección de procedimientos fundamentales titulada "Programas de identificación de clientes" (CIP por sus siglas en inglés) de la página 179 para obtener información adicional. Encontrará más información sobre las transacciones electrónicas en el *Manual de inspección de la tecnología de la información* del FFIEC.[110]

FACTORES DE RIESGO

Los bancos deben verificar que sus sistemas de monitoreo detecten adecuadamente las transacciones que se realicen electrónicamente. Como en cualquier cuenta, deben estar alerta a toda anomalía que presente la cuenta. Las señales de alarma [red flags] pueden incluir la velocidad con que ingresan fondos a la cuenta, o, en el caso de los cajeros automáticos, el número de tarjetas débito asociadas a la cuenta.

Las cuentas abiertas sin contacto cara a cara pueden implicar mayor riesgo de lavado de dinero y financiación 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 objetivo del banco.
. • El cliente puede percibir las transacciones como menos transparentes.
. • Las transacciones son instantáneas.

. • Pueden ser utilizadas por una empresa fachada o “testaferro” o terceros desconocidos.

FORMAS DE MITIGAR EL RIESGO

El *Manual de exámenes* [inspección] *de la tecnología de la información* del FFIEC se encuentra disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Los bancos deben establecer sistemas de monitoreo, identificación y reporte de la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML) para las actividades inusuales y sospechosas que se presenten en los sistemas de banca electrónica. Los sistemas de información gerencial útiles para detectar actividades inusuales en cuentas de alto riesgo incluyen informes de actividades en cajeros automáticos, informes de transferencia de fondos, informes de actividades de cuentas nuevas, informes de cambio de dirección de Internet, informes sobre direcciones de Protocolos de Internet (IP) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, direcciones, números telefónicos, direcciones de correo electrónico y números del identificación tributaria compartidos). Para determinar el nivel de monitoreo que requiere una cuenta bancaria, los bancos deben considerar entre varios factores la forma en que fue abierta la cuenta. Los bancos deben evaluar si los clientes que requieren ciertos servicios financieros tales como los de banca electrónica deban abrir sus cuentas cara a cara [compareciendo personalmente]. También pueden establecerse otros controles tales como fijar límites a las transacciones en dólares para montos elevados, de manera que se requiera una intervención manual para exceder el límite preestablecido.

Visión general ampliada – Transferencia de fondos

OBJETIVO

Evaluar si los sistemas bancarios son adecuados para administrar los riesgos asociados a la transferencia de fondos, y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes. Esta sección amplía la revisión fundamental de los requerimientos estatutarios y regulatorios de las transferencias de fondos para proporcionar una evaluación más amplia de los riesgos asociados a la actividad de lavado de dinero (AML).

VISIÓN GENERAL

En los Estados Unidos los sistemas de pago incluyen a numerosos intermediarios financieros, entidades de servicios financieros y empresas no bancarias que generan, procesan y distribuyen pagos. La ampliación nacional e internacional de la industria de operaciones bancarias y los servicios financieros no bancarios ha incrementado la importancia de las transferencias electrónicas de fondos, como la transferencia a través de sistemas de pago mayoristas. Para conocer más información sobre los sistemas de pago mayoristas, consultar el *Manual de exámenes* [inspección] *de la tecnología de la información* del FFIEC[111].

SERVICIOS DE TRANSFERENCIA DE FONDOS

La gran mayoría del valor que tienen los pagos efectuados en dólares estadounidenses en los Estados Unidos se procesa en última instancia a través de sistemas de pago mayoristas, que por lo general manejan transacciones de alto valor entre bancos y grandes proveedores de servicios financieros o entidades financieras no bancarias. En comparación, los sistemas de transferencia minorista incluyen cámaras de compensación automatizadas (ACH), los cajeros automáticos (ATM), sistemas de puntos de venta (POS), pago telefónico de cuentas, sistemas bancarios para el hogar, tarjetas débito y "tarjetas inteligentes", de uso cada vez más generalizado. La mayoría de estas transacciones minoristas las inician los clientes y no los bancos ni las corporaciones. Estas transacciones individuales pueden entonces combinarse para formar transferencias mayoristas más grandes, y éstas son las que interesan en esta sección. Además, los bancos realizan numerosas transferencias mayoristas en nombre propio, así como para beneficio de otros proveedores de servicios financieros y clientes bancarios (corporativos y clientes).

Los dos principales sistemas de pago de órdenes de pago de transferencias de fondos interbancarias o de alto valor nacionales son Fedwire[112] y Clearing House Interbank

[111] El *Manual de exámenes* [inspección] *de la tecnología de la información* del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html. [112] Fedwire® es una marca de servicio registrada de los Bancos de la Reserva Federal (*Federal Reserve Banks*). Para consultar más información ver www.frbservices.org/Wholesale/fedwirefunds.html.

Payment System [CHIPS].[113] La mayor parte del valor en dólares de estos pagos se procesa electrónicamente y se emplea para comprar, vender o financiar transacciones de títulos valores; desembolsar o pagar préstamos; liquidar transacciones de finca raíz; y hacer pagos de alto valor en los que el tiempo es un factor clave [time-critical payment], tales como pagos de liquidación de compras interbancarias y ventas de fondos federales, liquidación de transacciones de comercio exterior u otras transacciones del mercado financiero. Quienes usan Fedwire y CHIPS le facilitan estas transacciones a las entidades financieras no bancarias y a las empresas comerciales, así como a los bancos que no tienen acceso directo.

Estructuralmente las transferencias de fondos tienen dos componentes: las instrucciones, que contienen los datos del remitente y el destinatario final de los fondos, y el movimiento o transferencia real de los fondos. Las instrucciones se envían por diferentes vías incluyendo correo electrónico, fax, teléfono o télex; mediante acceso electrónico a las redes de los sistemas de pago Fedwire o CHIPS; y mediante acceso a los sistemas de telecomunicaciones financieras, como la Society for Worldwide Interbank Financial Telecommunication [Sociedad para las telecomunicaciones financieras interbancarias mundiales] (SWIFT). El sistema Fedwire se utiliza para las transferencias en dólares estadounidenses de transacciones enteramente nacionales y para facilitar la porción que va en dólares estadounidenses de las transacciones internacionales. El sistema CHIPS también puede usarse para transferencias enteramente nacionales en dólares de EE. UU. y para facilitar las transacciones internacionales, pero ha sido usado primordialmente para facilitar las transacciones internacionales. SWIFT es un servicio de mensajería internacional que se

usa para transmitir las instrucciones de pago de la gran mayoría de transacciones internacionales interbancarias, que están denominadas en muchos tipos de moneda.

Fedwire

El sistema Fedwire es operado por los Bancos de Reserva Federal y le permite a todo banco que tenga una cuenta en la Reserva Federal transferir fondos desde su cuenta a la cuenta de Reserva Federal de cualquier otro banco. El pago al participante receptor (beneficiario) a través de Fedwire es definitivo e irrevocable cuando el Banco de la Reserva Federal ya sea acredite el monto de la orden de pago a la cuenta de reserva del Banco de Reserva Federal del participante receptor o envíe una notificación al participante receptor, según lo que ocurra primero. Los participantes[114] pueden acceder al sistema Fedwire a través de los siguientes cuatro métodos:

[113]

CHIPS es un sistema de liquidación multilateral que pertenece a *The Clearing House Payments Company* y es operado por ésta.

[114] Los participantes en Fedwire son las entidades que mantienen una cuenta en el Banco de la Reserva Federal a nombre de la entidad. Sujetas a las políticas de reducción de riesgo del Banco de la Reserva Federal y la Junta de Gobernadores del Sistema de la Reserva Federal, cuando aplica, las entidades autorizadas por ley, regulación, política o contrato para ser participantes, incluyen las siguientes:

. • Instituciones de depósito.
. • Agencias y sucursales de bancos extranjeros.
. • Bancos miembros del Sistema de la Reserva Federal.
. • La Tesorería de los EE.UU y cualquier entidad específicamente autorizada por estatuto federal para usar los Bancos de Reserva Federal como agentes fiscales o de depósito.
. • Entidades designadas por la Secretaría del Tesoro.
. • Interfaz directa de computador
. • Por vía telefónica, fuera de línea, con el Banco de Reserva Federal
. • Por la web a través de una red virtual privada, a la cual puede accederse por Internet o mediante conexión de marcación.
. • Acceso de marcación a través de un sistema computarizado[115].

Aunque los participantes del sistema Fedwire no incurren el riesgo de liquidación [settlement risk], pueden estar expuestos a los riesgos de error, omisión y fraude.

CHIPS

CHIPS es un sistema de pagos multilateral administrado por particulares que opera en tiempo real y que se usa típicamente para el pago de grandes montos en dólares. El sistema CHIPS es de propiedad de los bancos, y toda organización bancaria con presencia regulada en los Estados Unidos puede convertirse en propietaria y participar en la red. Los pagos que se transfieren a través del sistema CHIPS con frecuencia corresponden a transacciones interbancarias internacionales, incluyendo los pagos en dólares que resultan de

transacciones en moneda extranjera (tales como contratos de intercambio de flujos de moneda [currency swap contracts]) y colocación de euros y retornos. También se pueden enviar órdenes de pago a través del sistema CHIPS para ajustar los saldos [de bancos] corresponsales y hacer pagos asociados a transacciones comerciales, préstamos bancarios y transacciones de títulos valores.

SWIFT

La red SWIFT es una infraestructura de mensajería que proporciona a los usuarios un enlace privado de comunicaciones internacionales entre ellos mismos. Los movimientos (pagos) en sí de fondos en dólares estadounidenses son logran a través de las relaciones bancarias de corresponsalía o de los sistemas Fedwire o CHIPS. Además de realizar transferencias de fondos de clientes y bancos, SWIFT se utiliza para transmitir confirmaciones de moneda extranjera, confirmaciones de ingresos de débitos y créditos, extractos o estados de cuenta, recaudos y créditos documentarios.

Sistemas informales de transferencia de valor

Por sistemas informales de transferencia de valor [IVTS por sus siglas en inglés] (por ejemplo, los "hawalas") se entienden los sistemas de negocios informales de transferencia de divisas o valores.[116] En los países que carecen de un sector financiero

. • Los bancos centrales extranjeros, autoridades monetarias extranjeras, gobiernos extranjeros, y ciertas organizaciones internacionales.
. • Todas las entidades autorizadas por el Banco de Reserva Federal para usar el Servicio de Títulos Valores de Fedwire.

Gradualmente los participantes del sistema Fedwire serán transferidos del sistema de discado computarizado al método de acceso a través de la web.

[116] Las fuentes de información sobre el sistema IVTS incluyen:
- FinCen Advisory 33 [Advertencia de FinCEN No. 23] *"Informal Value Transfer Systems"* [Sistemas informales de transferencia de valor] de marzo de 2003.

estable o que tienen grandes áreas no atendidas por bancos formales, el sistema IVTS puede ser el único método de realizar transacciones financieras. Las personas que viven en los Estados Unidos también pueden usar el sistema IVTS para transferir fondos a sus países de origen.

Pagadero contra identificación apropiada

Un tipo de transacción de transferencia de fondos que conlleva un riesgo particular es el servicio de pago contra identificación apropiada (PUPID por sus siglas en inglés). Las transacciones PUPID son transferencias de fondos en las que no existe una cuenta específica en la cual se consignan los fondos y el beneficiario de los fondos no es cliente del banco. Por ejemplo, una persona que tiene una cuenta en un banco puede transferir

fondos a un familiar o a una persona que no tiene una relación de cuenta con un banco en otra localidad (por ejemplo, ciudad, estado o jurisdicción). En este caso, el banco beneficiario puede colocar los fondos que ingresan en una cuenta provisional [suspense account] y finalmente entregar los fondos cuando la persona se identifique plenamente.

FACTORES DE RIESGO

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 usará el banco. La gran mayoría de las instrucciones de transferencia de fondos se envía electrónicamente; no obstante, los examinadores deben saber que las instrucciones físicas se pueden transmitir por otras vías informales, como las ya descritas.

Los IVTS [sistemas informales de transmisión de valor] plantean un problema serio porque pueden burlar el sistema formal. La ausencia de requisitos de registro aunada 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 con respecto a la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero (BSA/AML) porque permiten evadir los controles internos y la supervisión de monitoreo que caracterizan al sistema bancario formal. Los mandantes [principals] que operan sistemas IVTS con frecuencia usan los bancos para liquidar cuentas.

Los riesgos que implican las transacciones PUPID para los bancos beneficiarios son similares a los que tienen otras actividades en las que los bancos hacen transacciones con quienes no son clientes. Sin embargo, los riesgos son mayores con las transacciones PUPID porque el banco permite que una persona que no es cliente acceda al sistema de transferencias de fondos proporcionando mínima o ninguna información de identidad. Algunos bancos que permiten a no clientes transferir fondos usando 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 apenas tienen mínima

. • "Informe al Congreso sobre los Sistemas informales de transferencia de valor de conformidad con la Sección 359 de la Ley Patriota" del Tesoro de los EE. UU., noviembre de 2002.
. • "Nota interpretativa de la recomendación especial VI: Remisiones alternativas" de FATF [GAFI], junio de 2003.
. • "Lucha contra el abuso de los sistemas alternativos de remisiones, Mejores prácticas internacionales", de FATF [GAFI], octubre de 2002.

FORMAS DE MITIGAR EL RIESGO

Las transferencias de fondos pueden utilizarse en las etapas de colocación, estratificación (layering) 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 la actividad inusual en las etapas de estratificación e integración; tales transacciones pueden

parecer lícitas. En muchos casos, los bancos no participan en la colocación de los fondos o en la integración final, sino únicamente en la estratificación de las transacciones. Los bancos deben tomar en cuenta las tres etapas del lavado de dinero cuando se evalúan o estudian los riesgos de la transferencia de fondos.

Los bancos necesitan fijar políticas, procedimientos y trámites sólidos para manejar los riesgos de la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML) que tienen sus actividades de transferencia de fondos. Tales políticas pueden abarcar más que los requerimientos mínimos de registro de datos y expandirse para cubrir la OFAC [Oficina de control de activos extranjeros].

El riesgo que representan los servicios de transferencia de fondos se puede mitigar significativamente con la información proveniente de la debida diligencia del cliente (CDD). Debido a la naturaleza de las transferencias de fondos, las políticas, procedimientos y trámites de CDD adecuados son fundamentales para la detección de actividades inusuales y sospechosas. Igualmente importante es contar con un sistema eficaz y basado en riesgos para el monitoreo y reporte de operaciones sospechosas.

Los bancos originadores y los beneficiarios deben fijar políticas, procedimientos y procesos adecuados para las actividades PUPID que contemplen lo siguiente:

. • Especificación del tipo de identificación que se considera aceptable.
. • Mantenimiento de la documentación de los individuos conforme a las políticas de registro de datos del banco.
. • Definición de los empleados del banco que pueden realizar las transacciones PUPID.
. • Fijación de límites a los montos de fondos que pueden transferir desde y hacia los bancos quienes no son clientes (incluyendo el tipo de fondos que acepta (por ejemplo, moneda o cheques oficiales) el banco de origen.
. • Monitoreo y reporte de operaciones sospechosas.
. • Indagación más detallada para transferencias efectuadas desde y hacia ciertas jurisdicciones.

- Identificación de los métodos de desembolso (por ejemplo, en moneda o cheques oficiales) de los fondos provenientes del banco beneficiario.

Visión general ampliada – Efectivo electrónico

OBJETIVO

Evaluar si los sistemas bancarios son adecuados para manejar los riesgos asociados al dinero efectivo electrónico (e-cash o efectivo electrónico) y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

El dinero efectivo electrónico (e-cash) es una representación digital del dinero. El efectivo electrónico (también conocido como e-money o dinero electrónico) viene en dos presentaciones básicas: tarjeta de valor acumulado de efectivo electrónico [stored value card e-cash] y efectivo electrónico por computador [computer e-cash]. El efectivo electrónico de tarjeta de valor acumulado con frecuencia se descarga a través de Internet mediante terminales especiales (por ejemplo, cajeros automáticos (ATM), computadoras o teléfonos celulares especialmente equipados) y hacia tarjetas electrónicas. El efectivo electrónico de computador se descarga desde Internet al disco duro de un computador personal por medio de un módem o se guardado en un depósito en línea.

Los clientes usan el efectivo electrónico para acceder a fondos que se mantienen electrónicamente o guardarlos o redimirlos. La transferencia de fondos a la tarjeta es una forma de prepago (por ejemplo, las tarjetas de llamadas telefónicas). Además, actualmente el efectivo electrónico en presentación de tarjetas de nómina está siendo ofrecida por los empleadores a sus empleados en lugar de cheques para el pago de salarios. El valor de los fondos almacenados en estas tarjetas puede transferirse entre los proveedores y las personas que usan sistemas electrónicos compatibles, con frecuencia sin usar bancos.

Por medio de lectores especiales, el valor monetario almacenado es restado de la tarjeta. Cuando el valor monetario se agota, la tarjeta se descarta o en algunos casos su valor se reestablece. En el caso del dinero electrónico computarizado, el valor monetario se deduce de la cuenta bancaria cuando se hace una compra. En el *Manual de exámenes* [inspección] *de tecnología de la información* del FFIEC encontrará información adicional acerca de los tipos de productos de efectivo electrónico.[117]

FACTORES DE RIESGO

Las transacciones efectuadas con efectivo electrónico pueden plantear los siguientes riesgos particulares al banco:

- Los fondos pueden transferirse desde y hacia terceros desconocidos.

[117] El *Manual de examenes* [inspección] *de tecnología de la información* del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

- A medida que el efectivo electrónico es aceptado en todo el mundo, los clientes pueden evitar las restricciones fronterizas (border restrictions) puesto que las transacciones pueden tornarse móviles y no estar sujetas a las restricciones jurisdiccionales.
- Las transacciones son instantáneas.
- El cliente puede percibir las transacciones como menos transparentes.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben establecer sistemas de monitoreo, identificación y presentación de informes de Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML)

para las actividades inusuales y sospechosas que puedan ocurrir en los servicios de efectivo electrónico. Entre los sistemas de información de gestión [management information systems] que son útiles para detectar actividad inusual en cuentas de alto riesgo están los informes sobre actividad en cajeros automáticos (ATM) (enfocados en transacciones en el extranjero), informes sobre transferencias de fondos, informes sobre actividad de cuentas nuevas, informes sobre cambio de dirección de Internet, informes sobre la dirección del Protocolo de Internet (IP) e informes para identificar cuentas relacionadas o vinculadas (por ejemplo, con direcciones, números telefónicos, direcciones de correo electrónico y números de identificación tributaria compartidos). Los bancos también pueden aplicar otros controles, tales como ponerle límites a las transacciones y cuentas en dólares que requieran intervención manual para exceder los límites preestablecidos.

Visión general ampliada – Terceros que son procesadores de pagos

OBJETIVO

Evaluar si los sistemas bancarios son adecuados para manejar los riesgos que presentan sus relaciones con terceros procesadores de pagos, y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Los terceros no bancarios que procesan pagos son clientes del banco que proporcionan servicios de tramitación de pagos a comerciantes y a otras entidades comerciales.

Tradicionalmente los procesadores [de pagos] han celebrado contratos principalmente con minoristas que cuentan con instalaciones físicas para procesar sus transacciones. Estas transacciones de comerciantes principalmente consistían en pagos de tarjetas de crédito y también cubrían transacciones en cheques o giros a la vista [demand drafts] de cámaras de compensación automatizadas[118] (también conocidos como e-checks o cheques electrónicos) y transacciones de tarjetas débito o de valor acumulado. Con la ampliación de Internet se eliminó la separación constituida por los minoristas. Los procesadores ahora prestan servicios a toda una variedad de cuentas comerciales, incluyendo a establecimientos minoristas convencionales y aquellos basados en Internet, viajes prepagados y empresas de juegos por Internet.

FACTORES DE RIESGO

Por lo general, los procesadores no están sujetos a los requerimientos regulatorios de la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML). Como resultado, algunos procesadores pueden ser utilizados para el lavado de dinero, hurto de identidad y esquemas fraudulentos.

Los riesgos BSA/AML que corren los bancos cuando tratan con cuentas de procesadores son similares a los que presentan otras actividades en las cuales el cliente del banco realiza transacciones en el banco en nombre de los clientes del cliente. Cuando el banco no puede identificar y no conoce la naturaleza y fuente de las transacciones que se procesan a través de una cuenta, pueden aumentar los riesgos para el banco y la probabilidad de una actividad sospechosa. Si el banco no ha implementado un programa adecuado de aprobación de procesador [de pagos] más allá de lo permite la gestión del riesgo crediticio [credit risk management], puede ser vulnerable al procesamiento de transacciones ilícitas o sancionadas.

FORMAS DE MITIGAR EL RIESGO

[118] Un cheque o giro a la vista [demand draft] es un sustituto del cheque preimpreso en papel. El giro se realiza sin la firma del cliente pero presumiblemente con su autorización.

Los bancos que ofrecen servicios de cuenta a procesadores deben fijar y mantener políticas, procedimientos y procesos adecuados para enfrentar los riesgos inherentes a estas relaciones. Como mínimo, estas políticas deben autenticar las operaciones comerciales del procesador y evaluar su nivel de riesgo. Se puede verificar y evaluar a los procesadores mediante los siguientes procedimientos:

. • Revisión de los materiales de promoción del procesador, incluyendo su sitio web, para determinar su clientela objetivo (los negocios de elevado riesgo pueden incluir empresas extraterritoriales, operaciones relacionadas con juegos en línea, y prestamistas del día de pago [pay day lenders] en línea). Por ejemplo, un procesador cuyos clientes son principalmente extraterritoriales tendrá inherentemente más riesgo que un procesador cuyos clientes son principalmente restaurantes.

. • Determinación de si el procesador revende sus servicios a un tercero que puede ser conocido como un "agente o proveedor de oportunidades de Organización de ventas independiente (ISO) [Independent Sales Organization] o acuerdos "gateway"[119].

. • Revisión de las políticas, procedimientos y procesos del procesador para determinar la idoneidad de sus estándares de la debida diligencia para nuevos comerciantes.

. • Identificación de los clientes principales del procesador.

. • Revisión de la documentación corporativa incluyendo los servicios independientes de elaboración de informes y si aplica, la documentación de los propietarios principales.

. • Visita al centro de operaciones del negocio del procesador.

Los bancos que proporcionan servicios de cuentas deben monitorear las relaciones de su procesador, buscando cualquier cambio significativo en sus estrategias de negocio que pueda afectar su perfil de riesgo. Los bancos deben periódicamente verificar de nuevo y actualizar los perfiles del negocio para asegurarse de que la evaluación del riesgo es adecuada.

Además de realizar una apertura de cuenta adecuada y eficaz, y los procedimientos de

debida diligencia a las cuentas del procesador, la gerencia debe vigilar estas relaciones en busca de actividades inusuales o sospechosas. Para monitorear eficazmente estas cuentas el banco debe conocer la siguiente información sobre el procesador:

. • Base del comerciante.
. • Actividades del comerciante.
. • Volumen promedio en dólares y número de transacciones.
. • Volumen "de barrido" ["swiping" volume] comparado con el volumen "de digitación" ["keying" volume] en transacciones de tarjetas de crédito.

[119] Los acuerdos "gateway" [o tipo portal de acceso] son similares a los de los proveedores de Internet que tienen exceso de capacidad de almacenamiento computarizado, los cuales venden esta capacidad a terceros, quienes a su vez distribuyen los servicios de computación a otras personas que son desconocidas para el proveedor. El tercero decide quién recibe el servicio, aunque el proveedor es quien aporta la capacidad final de almacenamiento. Por tanto, el proveedor asume todos los riesgos y recibe menos ganancias.

• Antecedentes de devoluciones o descuentos [charge-back].

Visión general ampliada – Compra y venta de instrumentos monetarios

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a los instrumentos monetarios y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes. Esta sección amplía la revisión fundamental de los requerimientos estatutarios y regulatorios para la compra y venta de instrumentos monetarios con el fin de proporcionar una evaluación más amplia de los riesgos de lavado de dinero asociados a esta actividad.

VISIÓN GENERAL

Los instrumentos monetarios son productos que ofrecen los bancos e incluyen cheques de gerencia, cheques viajeros y giros postales. Los instrumentos monetarios típicamente se compran para pagar transacciones comerciales o personales, y en el caso de los cheques viajeros, como una fuente de valor acumulado para compras futuras.

FACTORES DE RIESGO

La compra o el intercambio de instrumentos monetarios en las etapas de colocación y estratificación del lavado de dinero, pueden ocultar el origen de los activos ilícitos. Como resultado, los bancos han sido los objetivos principales de las operaciones de lavado porque proporcionan y procesan instrumentos monetarios a través de depósitos (consignaciones). Por ejemplo, se ha sabido que clientes y no clientes compran instrumentos monetarios por valores inferiores al umbral de US $ 3.000 para evitar tener que proporcionar una identificación adecuada. Después, los instrumentos monetarios se colocan en cuentas de

depósito para evadir el umbral de radicación del Informe de transacciones en moneda (CTR) [Currency Transaction Report].

FORMAS DE MITIGAR EL RIESGO

Los bancos que venden instrumentos monetarios deben fijar políticas, procedimientos y trámites adecuados para mitigar el riesgo. Las políticas deben definir lo siguiente:

. • Las transacciones de instrumentos monetarios que son aceptables y que no lo son (por ejemplo, las transacciones de quienes no son clientes, instrumentos monetarios en donde el beneficiario aparece en blanco, instrumentos monetarios sin firma, requerimientos de identificación para transacciones estructuradas o la compra múltiple y secuencial de instrumentos monetarios para el mismo beneficiario).
. • Los procedimientos de revisión para actividades inusuales o sospechosas, incluyendo remitir los problemas a la gerencia.
. • Los criterios para cerrar las relaciones o rehusarse a negociar con personas que no son clientes y consistentemente o de manera muy notoria han participado en una actividad sospechosa.

Visión general ampliada – Depósitos a través de intermediarios

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las relaciones de depósitos a través de intermediarios y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

El uso de los depósitos a través de intermediarios es una fuente común de fondos en muchos bancos. Recientes desarrollos tecnológicos permiten que los intermediarios proporcionen a los bancos mayor acceso a una amplia gama de inversionistas potenciales que no tienen una relación con el banco. Los depósitos se pueden obtener a través del Internet, de servicios de listas de certificados de depósito o a través de otros métodos de publicidad.

La intermediación para depósitos le sirve a bancos e inversionistas. Se considera que esta actividad es de mayor riesgo porque cada intermediario procede según sus propias pautas para conseguir depósitos. El nivel de supervisión regulatoria que cobija a los intermediarios de depósitos varía, así como la aplicabilidad directa de los requerimientos BSA/AML sobre el intermediario depositante. Sin embargo, el intermediario depositante está sujeto a los requerimientos de la OFAC (Oficina de Control de Activos Extranjeros) independientemente de su estado regulatorio. Por lo tanto es posible que el intermediario no

practique adecuadamente la debida diligencia, la detección sistemática OFAC (para consultar información adicional lea la sección de visión general fundamental titulada "Oficina de Control de Activos en el Exterior" en la página 84) o los procedimientos del Programa de Identificación del Cliente (CIP por sus siglas en inglés). La aceptación de los bancos de los depósitos hechos a través de intermediarios depende de que el intermediario haya practicado suficientes procedimientos de apertura de cuenta y siga los requerimientos aplicables del programa de cumplimiento BSA/AML.

FACTORES DE RIESGO

Los riesgos de lavado de dinero y financiación del terrorismo se presentan porque el banco posiblemente no conoce a los propietarios finales de los fondos ni su origen. El intermediario podría representar a un rango de clientes con alto riesgo de lavado de dinero y financiación del terrorismo (por ejemplo, clientes no residentes o extraterritoriales, personas expuestas políticamente o bancos extranjeros ficticios [shell banks])

FORMAS DE MITIGAR EL RIESGO

Los bancos que aceptan cuentas o fondos de intermediarios deben fijar políticas, procedimientos y trámites adecuados que establezcan procedimientos mínimos de CDD para todos los intermediarios que realicen depósitos en el banco. El nivel de debida diligencia que practique un banco debe ser proporcional a su conocimiento del intermediario y de las prácticas comerciales y base de clientes del mismo.

Para enfrentar el riesgo inherente a las relaciones con intermediarios de depósitos, los bancos deben tener contrato firmado que fije las funciones y responsabilidades de cada una de las partes así como las restricciones por tipos de clientes (por ejemplo, los clientes no residentes o extraterritoriales, las personas expuestas políticamente o los bancos extranjeros ficticios). Los bancos deben practicar la debida diligencia a los intermediarios de depósito que son desconocidos, extranjeros, independientes o no están regulados. Para manejar los riesgos BSA/AML asociados a los depósitos hechos por intermediarios, el banco debe llevar a cabo lo siguiente:

- Determinar si el intermediario es una empresa legal, en todas las localidades donde opera.
- Revisar las estrategias de negocio del intermediario, incluyendo los mercados de clientes objetivo (por ejemplo, clientes extranjeros o nacionales) y los métodos para buscar clientes.
- Determinar si el intermediario está sujeto a supervisión regulatoria.
- Evaluar si las políticas, procedimientos y procesos BSA/AML/OPAC del intermediario son adecuados (por ejemplo, verificar si el intermediario practica suficiente debida diligencia (CDD) incluyendo procedimientos CIP).
- Determinar si el intermediario practica una detección sistemática de clientes para verificar correspondencias [o concordancias] con las listas de la OFAC.
- Evaluar la idoneidad de las auditorias BSA/AML/OPAC del intermediario y asegurarse de que éstas incluyan el cumplimiento de las regulaciones y requerimientos aplicables.

.Los bancos deben tener especial cuidado en su supervisión de los intermediarios que no son entidades reguladas y que además:

- Son desconocidos para el banco.
- Practican negocios u obtienen depósitos principalmente en otras jurisdicciones.
- Usan empresas y bancos con los cuales es difícil comunicarse para averiguar referencias.
- Brindan otros servicios que pueden ser sospechosos, como crear empresas ficticias para clientes extranjeros.
- Se niegan a proporcionar la información de auditoria y debida diligencia solicitada, o insisten en colocar depósitos antes de suministrar la mencionada información.
- Usan tecnología que proporciona anonimato a los clientes.

Los bancos también deben vigilar las relaciones que tengan con intermediarios de depósitos, en busca de cualquier cambio significativo en las estrategias de negocios que pueda influir en el perfil de riesgo del intermediario. Así, los bancos deben verificar y actualizar periódicamente el perfil de cada intermediario para asegurar una evaluación de riesgo adecuada.

Visión general ampliada – Cajeros automáticos de propiedad privada

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a los cajeros automáticos de propiedad privada y las relaciones con organizaciones de ventas independientes (ISO – Independent Sales Organizations), así como la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Los cajeros automáticos de propiedad privada son especialmente susceptibles al lavado de dinero y el fraude. Los operadores de estos cajeros automáticos con frecuencia se incluyen en la definición de las ISO.[120]

Los cajeros automáticos de propiedad privada típicamente se encuentran en “rapitiendas” [convenience stores], bares, restaurantes, tiendas de abarrotes o establecimientos de cambio de cheques. Algunas ISO son operadores de gran escala, pero los propietarios de muchos cajeros automáticos de propiedad privada son los mismos dueños de los establecimientos en los que están localizados. La mayoría dispensan dinero en efectivo, pero algunos sólo dispensan un recibo de papel (vale) que el cliente cambia por dinero o artículos. Los honorarios y sobrecargos por los retiros, aunados a los negocios adicionales generados por el acceso de un cliente a un cajero automático, hacen que la operación de un cajero automático de propiedad privada sea rentable.

Las ISO vinculan sus cajeros automáticos a una red de transacciones de los mismos. La red de cajeros automáticos envía los datos de las transacciones al banco del cliente para debitarlos de la cuenta del cliente y finalmente acreditar los montos a la cuenta de la ISO, la cual puede estar ubicada en cualquier banco del mundo. Los pagos a la cuenta de la ISO típicamente los hace el sistema ACH. El *Manual de exámenes* [inspección] *de la tecnología de la información* del FFIEC tiene información adicional sobre los tipos de sistemas de pago al detal.[121]

Banco patrocinador

[120] Las ISO típicamente actúan como agentes de los comerciantes, incluyendo a 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 de ISO. Los bancos pueden contratar los servicios de una ISO para buscar comerciantes y cajeros automáticos de propiedad privada; no obstante, en muchas situaciones, la ISO celebra un contrato con los comerciantes y los propietarios de los cajeros automáticos sin la revisión y la aprobación del banco de compensación.

[121] El *Manual de exámenes* [inspección] *de la tecnología de la información* del FFIEC está disponible en www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

Algunas transferencias electrónicas de fondos (EFT por su sigla en inglés) o redes de puntos de venta (POS por sus siglas en inglés) requiere que la ISO esté patrocinada por algún miembro de la red (banco patrocinador). El banco patrocinador y la ISO están sujetos a todas las reglas de la red. El banco patrocinador también está encargado de asegurar que la ISO cumpla con todas las reglas de la red. Por tanto, el banco patrocinador debe realizar una debida diligencia adecuada a la ISO y mantener la documentación adecuada para asegurar que la ISO patrocinada cumpla con las reglas de la red.

FACTORES DE RIESGO

Actualmente la mayor parte de los estados [de Estados Unidos] no registra los cajeros automáticos de propiedad privada ni sus ISO, ni fija límites a propiedad de los mismos ni a su monitoreo o inspección. Si bien el proveedor de la red de transacciones del cajero automático y el banco patrocinador deben realizar una debida diligencia adecuada a la ISO, en la realidad las prácticas varían. Además, es posible que el proveedor no esté enterado de los cambios que se hayan dado en la propiedad del cajero automático o la ISO una vez firmado el contrato con el cajero automático. Como consecuencia de esto muchos cajeros automáticos de propiedad privada han participado en estratagemas de lavado de dinero, hurto de identidad, robo escueto de dinero y fraude, o son susceptibles a todo ello. Por lo tanto los cajeros automáticos de propiedad privada y sus ISO implican un mayor riesgo y por consiguiente deben ser tratados de manera acorde por los bancos que negocian con ellos.

Algunos cajeros automáticos de propiedad privada son manejados por servidores de moneda para bóvedas [vault currency servicer], los cuales entregan el dinero en vehículo

blindado, reabastecen los cajeros automáticos y los aseguran contra robo y daños. No obstante, muchas ISO administran y le hacen mantenimiento a sus propias máquinas e incluso las abastecen con dinero. Los bancos también pueden suministrar dinero a las ISO mediante contratos de préstamo, lo que expone a esos bancos a distintos riesgos, inclusive el riesgo de afectar su reputación y su crédito.

El lavado de dinero puede hacerse a través de cajeros automáticos de propiedad privada cuando algunos de éstos se reabastecen con dinero ilegal que luego es retirado por clientes legales. Este proceso se convierte en depósitos ACH en la cuenta ISO que aparecen como transacciones comerciales lícitas. Por consiguiente las tres fases del lavado de dinero (colocación, estratificación e integración) pueden darse simultáneamente. Los lavadores de dinero pueden también confabularse con los comerciantes y las ISO que antes eran lícitas, para abastecer los cajeros automáticos con dinero ilícito a cambio de un descuento.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben implementar políticas, procedimientos y procesos adecuados para enfrentar los riesgos que presentan las relaciones con las ISO. Como mínimo dichas políticas deben incluir lo siguiente:

. • Verificación de la legitimidad de la ISO mediante una revisión de la documentación, licencias, permisos, contratos o referencias de la corporación.
. • Revisión de las bases de datos públicas para determinar la existencia de problemas con la ISO o sus propietarios principales.
. • Conocer los contratos celebrados con los servicios de entrega de dinero a los cajeros automáticos privados, y si el dinero legítimo generado es suficiente para servir las máquinas.
. • Revisión de la documentación de ubicación de los cajeros automáticos privados y determinación del mercado objetivo de la ISO según la ubicación geográfica.
. • Actividad esperada de la cuenta, incluyendo retiros de dinero.

Debido a estos riesgos, es fundamental realizar la debida diligencia en clientes que son Organizaciones independientes de ventas (ISO), más allá de los requerimientos mínimos del Programa de identificación del cliente. Los bancos también deben realizar la debida diligencia a los propietarios de los cajeros automáticos. La mencionada debida diligencia debe incluir lo siguiente:

. • Verificar la legalidad del propietario del cajero automático mediante una revisión de la documentación, licencias, permisos, contratos o referencias de la corporación, incluyendo el contrato del proveedor de transacciones del cajero automático.
. • Revisar las bases de datos públicas para buscar información sobre los propietarios de los cajeros automáticos.
. • Obtener las direcciones de todas las ubicaciones de los cajeros automáticos, comprobar los tipos de negocios donde estén localizados e identificar la población objetivo.
. • Determinar los niveles de actividad esperados del cajero automático, incluyendo retiros de dinero.

. • Determinar las fuentes de dinero para los cajeros automáticos mediante la revisión de copias de los contratos del vehículo blindado, los contratos de préstamos o cualquier otra documentación, según sea adecuado.

Visión general ampliada – Productos de inversión de no depósito [nondeposit]

OBJETIVO

Evaluar si los sistemas de los bancos son adecuados para manejar los riesgos asociados a los productos de inversión de no depósito (NDIP por sus siglas en inglés) que existen en la red o en el banco, y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Los productos de inversión de no depósito (NDIP) incluyen un amplio rango de productos de inversión (por ejemplo, títulos valores, bonos, anualidades fijas o variables). Los programas de venta también pueden incluir cuentas de barrido [o reinversión automática de fondos inactivos – "sweep accounts"] de manejo de efectivo para clientes minoristas y comerciales, en programas que los bancos ofrecen directamente. Los bancos ofrecen estas inversiones para aumentar sus ingresos por tarifas y comisiones y proporcionar a los clientes productos y servicios adicionales. La manera en que está estructurada la relación de los productos de inversión de no depósito (NDIP) y los métodos mediante los cuales se ofrecen, afectan considerablemente los riesgos y responsabilidades BSA/AML del banco.

Acuerdos de operación en red

Los bancos típicamente celebran acuerdos de operación en red con agentes e intermediarios de títulos valores, para ofrecer NDIP en las instalaciones de los bancos. Para los propósitos de la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML), en los acuerdos de operación en red el cliente es cliente del agente o intermediario, aunque el cliente también puede ser cliente del banco en otros servicios financieros. Los examinadores del banco reconocen que la Comisión de Vigilancia y Control del Mercado de Valores de EE. UU. (SEC) [Securities and Exchange Commission] es el principal regulador de la oferta de NDIP por medio de agentes e intermediarios y las agencias cumplirán con los requerimientos de supervisión funcional de la Ley Gramm-Leach-Biley.[122] Las agencias bancarias federales están encargadas de supervisar las actividades NDIP realizadas directamente por los bancos.

[122] La regulación funcional limita las circunstancias en las cuales las agencias de operaciones bancarias federales pueden inspeccionar directamente o requerir informes de una sucursal o filial bancaria cuyo regulador principal es la SEC [Comisión de Vigilancia y Control del Mercado de Valores], la Comisión de Comercio en Futuros de Productos Básicos [Commodity Futures Trading Commission], o las autoridades

estatales de emisión. Las agencias federales de operaciones bancarias por lo general están impedidas para inspeccionar a esas entidades, salvo si se requiere más información para determinar si la sucursal o filial bancaria representa un riesgo material para el banco, para determinar el cumplimiento de algún requisito legal bajo la jurisdicción de las agencias bancarias federales, o para evaluar el sistema de gestión de riesgo del banco encargado de las actividades que están funcionalmente reguladas. Estos estándares requieren mayor dependencia en el regulador funcional y mejor colaboración entre los reguladores.

Productos de marca conjunta [co-branded products] – Los productos de marca conjunta los ofrece otra empresa o corporación de servicios financieros[123] en copatrocinio con el banco. Por ejemplo, una corporación de servicios financieros crea un producto de fondo mutuo para vender en un banco específico. El producto es vendido exclusivamente en el 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 la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML) se vuelve compleja. Puesto que el control de estas cuentas no radica únicamente los bancos o las entidades financieras, la responsabilidad de realizar la debida diligencia del cliente (CCD), el Programa de identificación del cliente (CIP) y el monitoreo y reporte de operaciones sospechosas, puede variar. Los bancos deben conocer plenamente las responsabilidades contractuales de cada parte y asegurar un control adecuado de todas las partes.

Acuerdos de un empleado compartido – En un programa de empleado compartido, el banco y una corporación de servicios financieros, como por ejemplo una agencia de seguros o un agente o intermediario registrado, tienen un empleado común (compartido). El empleado compartido puede encargarse de negocios bancarios y también vender NDIP, o vender NDIP de tiempo completo. Debido a este acuerdo de empleado compartido, el banco tiene la responsabilidad de las actividades NDIP. Incluso si los acuerdos contractuales establecen que la corporación de servicios financieros es responsable de la BSA/AML, el banco sigue siendo responsable y debe asegurar una supervisión adecuada y el cumplimiento de todos los requerimientos regulatorios.[124]

Bajo algunos acuerdos de operación en red, los representantes de ventas registrados de títulos valores son empleados compartidos del banco y del agente o intermediario. Cuando el empleado compartido está ofreciendo productos y servicios de inversión, el agente o intermediario se encarga de verificar el cumplimiento del representante de ventas registrado con las leyes y la regulación de títulos valores aplicables. Cuando el empleado compartido ofrece productos y servicios bancarios, el banco tiene la responsabilidad de vigilar el desempeño y el cumplimiento del empleado con respecto a la BSA/AML.

Acuerdos con terceros – Los acuerdos con terceros pueden comprender el arriendo de espacio en el vestíbulo del banco a una corporación de servicios financieros para vender NDIP. En este caso el tercero debe diferenciarse claramente del banco. Si el acuerdo se implementa correctamente, los arreglos con terceros no afectan los requisitos de cumplimiento BSA/AML del banco. Como una buena práctica, se recomienda a los

[123] Las corporaciones de servicios financieros incluyen entidades que ofrecen NDIP, lo que puede incluir empresas de inversión, instituciones financieras, intermediarios/distribuidores de títulos valores y compañías de seguros.

[124] Si el banco usa la disposición de dependencia del CIP, la responsabilidad por el CIP se traslada al tercero proveedor. Consulte la sección de visión general fundamental titulada "Programa de identificación del cliente [CIP]" en la página 30 para obtener información adicional.

Ventas en el banco y productos de propiedad exclusiva [proprietary products]

A diferencia de los acuerdos de operación en red, el banco es concretamente responsable por las transacciones NDIP efectuadas en el banco a nombre de sus clientes, con o sin el beneficio de un empleado interno del agente o intermediario.[125] Además, el banco también puede ofrecer sus propios NDIP de propiedad exclusiva, los cuales pueden crear y ofrecer el banco, sus subsidiarias o afiliadas.

Con las ventas en el banco [in-house sales] y los productos de propiedad exclusiva, es posible que la totalidad de la relación con el cliente y todos los riesgos BSA/AML deban ser manejados por el banco, dependiendo de cómo se venden los productos. A diferencia de los acuerdos de operación en red, en los cuales todas o algunas responsabilidades pueden ser asumidas por el tercero agente o intermediario, con las ventas en el banco y los productos de propiedad exclusiva el banco debe manejar todas sus ventas NDIP logradas en el banco y sus productos de propiedad exclusiva no solo a nivel de sus departamentos, sino para toda la empresa en general.

FACTORES DE RIESGO

Los riesgos BSA/AML se presentan porque los NDIP pueden comprender arreglos jurídicos complejos, montos elevados en dólares y rápidos movimientos de fondos. Los portafolios NDIP que administran y controlan directamente los clientes plantean un mayor riesgo de lavado de dinero que los que administran los bancos o proveedores de servicios financieros. Los clientes sofisticados pueden llegar estructurar la propiedad de tal forma que quedan ocultos el control final y la propiedad de estas inversiones. Por ejemplo, los clientes pueden retener cierto nivel de anonimato constituyendo Sociedades de inversión privada (PIC por sus siglas en inglés), sociedades fiduciarias extraterritoriales u otras entidades de inversión que ocultan la propiedad o la participación del beneficiario propietario.

FORMAS DE MITIGAR EL RIESGO

La gerencia debe fijar políticas, procedimientos y trámites basados en riesgos, que le permitan al banco identificar relaciones y circunstancias de cuenta inusuales, activos y

[125] No se considerará que un banco es un agente o intermediario, ni que requiere tener un empleado registrado como agente o intermediario, porque el banco participa en una o más de las [siguientes] actividades bajo las respectivas condiciones:

. • El banco hace transacciones de clientes en títulos valores municipales.
. • El banco no realiza más de quinientas (500) transacciones en títulos valores para sus clientes en un año calendario dado, y dichas transacciones no las hace un empleado del banco que también es empleado del agente o intermediario.
. • El banco negocia en papeles comerciales, aceptaciones bancarias, letras comerciales o títulos valores exentos.
. • El banco realiza transacciones de clientes en productos bancarios identificados según la sección 206 de la Ley Gramm-Leach-Bliley.
. • El banco realiza transacciones de clientes en ciertos planes de compra de acciones, tales como planes de beneficios para empleados, planes de reinversión de dividendos y planes de emisor.

fuentes de fondos cuestionables y otras áreas potenciales de riesgo (por ejemplo, cuentas extraterritoriales, cuentas en agencias y beneficiarios no identificados). La gerencia debe mantenerse alerta a las situaciones que requieran una revisión o investigación más profunda.

Acuerdos de operación en red

Antes de celebrar un acuerdo de operación en red, los bancos deben realizar una revisión adecuada del agente o intermediario. La revisión debe incluir una evaluación del estado financiero del mismo y de su experiencia gerencial, estado de su vinculación con la Asociación Nacional de Operadores en Valores o Bolsa (NASD por sus siglas en inglés), reputación y habilidad para observar las responsabilidades de cumplimiento BSA/AML con respecto a los clientes minoristas del banco. Una debida diligencia adecuada incluiría una determinación de que el agente o intermediario cuenta con políticas, procedimientos y procesos adecuados para cumplir con sus obligaciones legales.

El banco debe mantener documentación de su debida diligencia del agente o intermediario. Además, todos los aspectos relativos al acuerdo de operación en red deben estar contemplados en detalle en un contrato, incluyendo las responsabilidades del agente o intermediario y sus representantes registrados. El contrato debe cubrir específicamente las responsabilidades de cada parte respecto al cumplimiento de las regulaciones y leyes BSA/AML y del monitoreo y reporte de las operaciones sospechosas.

Los bancos también podrán mitigar su exposición al riesgo limitando ciertos productos de inversión únicamente a sus clientes minoristas. Los productos de inversión tales como las PIC, sociedades fiduciarias extraterritoriales o fondos de cobertura extraterritoriales pueden implicar transferencias internacionales de fondos u ofrecer a los clientes formas de ocultar la propiedad.

La gerencia del banco debe hacer esfuerzos razonables para actualizar su información de debida diligencia de los agentes o intermediarios. Tales esfuerzos pueden incluir revisiones periódicas de los datos sobre el cumplimiento de los agentes o intermediarios con sus responsabilidades BSA/AML, verificación de sus antecedentes de cumplimiento con las pruebas y una revisión de las quejas de los clientes. También se recomienda a los gerentes bancarios, siempre que sea posible, revisar los informes BSA/AML generados por el agente o intermediario. Esta revisión puede incluir información sobre apertura de cuentas, transacciones, productos de inversión vendidos y monitoreo y reporte de operaciones

sospechosas.

Ventas en el banco y productos de propiedad exclusiva

La gerencia del banco debe evaluar el riesgo según diferentes factores tales como los siguientes:

. • Tipo de NDIP comprados y el tamaño de las transacciones.
• Tipos y frecuencia de las transacciones.
• País de residencia de los mandantes o beneficiarios, o el país de constitución o fuente de los fondos.
. • Cuentas y transacciones que no son usuales o acostumbradas por el cliente o el banco.

Para los clientes que la gerencia considera de alto riesgo de lavado de dinero y financiación del terrorismo, se debe establecer una documentación más estricta, verificación y procedimientos de monitoreo de las transacciones. Puede ser adecuado realizar una debida diligencia mejorada, en las siguientes situaciones:

. • Al iniciar el banco una relación nueva con un cliente.
. • Las cuentas no discrecionales registran 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 riesgo más alto.
. • Los activos y las transacciones son atípicas para el cliente.
. • El tipo de inversiones, tamaño, activos o las transacciones son atípicas para el banco.
. • Las transferencias internacionales de fondos se realizan especialmente desde fuentes de fondos extraterritoriales.
. • La identidad de los mandantes o beneficiarios de las inversiones o relaciones no se conoce o no se puede establecer fácilmente.
. • En las inversiones o transacciones son partes personas políticamente expuestas.

Visión general ampliada – Seguros

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a la venta de seguros, y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Los bancos venden seguros para aumentar su rentabilidad, principalmente ampliando y diversificando sus ingresos por comisiones y tarifas. Los productos de seguros típicamente se venden a clientes del banco a través de acuerdos de operación en red con afiliadas, operadoras subsidiarias u otros terceros proveedores de seguros. Los bancos también están interesados en proporcionar oportunidades de ventas cruzadas a los clientes, ampliando así los seguros que ofrecen. Los productos de seguros que venden incluyen vida, salud, propiedad y accidentes y anualidades fijas o variables.

FACTORES DE RIESGO

Los seguros se prestan para el lavado de dinero. Por ejemplo, se compran una o más pólizas de seguros de vida con dinero, que luego el tenedor rápidamente cancela (procedimiento conocido como "amortización anticipada" [early surrender]) a cambio de una multa. La compañía de seguros reembolsa el dinero al comprador mediante un cheque. Las pólizas de seguros que no son de vida pueden usarse para lavar dinero o financiar el terrorismo si el tenedor presenta reclamaciones infladas o falsas al asegurador. Si éstas se pagan, le permiten al asegurado recuperar parte o la totalidad de los pagos originalmente invertidos. Otras formas de usar los seguros para lavar dinero son:

- Préstamos contra el valor de rescate en efectivo [cash surrender value] de las pólizas de seguros de vida permanentes.
- Venta de unidades en productos asociados a la inversión (tales como anualidades).
- Utilización de los fondos del valor de rescate anticipado de una póliza anterior para comprar otros activos financieros.
- Compra de pólizas que permiten transferir el usufructo de las mismas sin el conocimiento ni el consentimiento del emisor (por ejemplo, "endowment" [o seguros mixtos] de segunda mano y pólizas al portador).[126]

FORMAS DE MITIGAR EL RIESGO

Consulte la "Documento guía sobre la lucha contra el lavado de dinero y la financiación del terrorismo" de la Asociación Internacional de Supervisores de Seguros [International Association of Insurance Supervirors], de octubre de 2004. Disponible en www.iaisweb.org.

- Identificación de las cuentas de alto riesgo.
- Realización de la debida diligencia del cliente, incluyendo debida diligencia ampliada a las cuentas de mayor riesgo.
- Productos, servicios y mercados objetivo.
- Compensación y bonificaciones de empleados relacionadas con las ventas.
- Monitoreo, incluyendo revisión de la terminación anticipada de pólizas y reporte de operaciones inusuales o sospechosas (por ejemplo, un pago de prima único y elevado, compra de un producto que parece estar por fuera del rango normal de las

transacciones financieras de un cliente, rescate o redención anticipada, transacciones múltiples, pagos a terceros aparentemente no relacionados y préstamos respaldados con garantía).

. • Registro de datos.

Visión general ampliada – Cuentas de concentración

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las cuentas de concentración, y la capacidad de la gerencia para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Las cuentas de concentración son cuentas internas establecidas para facilitar la tramitación y liquidación de transacciones múltiples o individuales de los clientes en el banco, usualmente el mismo día. Estas cuentas también se conocen como cuentas de uso especial, cuentas ómnibus, cuentas puente o de tránsito, de liquidación, intradía [intraday], de barrido o de cobro. A menudo se utilizan para facilitar las transacciones de la banca privada, cuentas de fideicomisos y cuentas de custodia de valores, transferencias de fondos y afiliadas internacionales.

FACTORES DE RIESGO

El riesgo de lavado de dinero puede presentarse en las cuentas de concentración si la identificación del cliente, como por ejemplo su nombre, el monto de la transacción y el número de la cuenta, se separan de la transacción financiera en sí. Esta separación permite perder el rastro de auditoria y las cuentas pueden ser usadas o administradas de forma indebida. Los bancos que utilizan las cuentas de concentración deben implementar políticas, procedimientos y procesos adecuados para cubrir las operaciones y los registros de estas cuentas. Las políticas deben establecer pautas para identificar, medir, monitorear y controlar los riesgos.

FORMAS DE MITIGAR LOS RIESGOS

Por los riesgos involucrados, la gerencia debe estar familiarizada con la naturaleza de los negocios de sus clientes y las transacciones que pasan por las cuentas de concentración del banco. También se requiere vigilar las transacciones de las cuentas de concentración para identificar y reportar operaciones inusuales o sospechosas.

Los controles internos se requieren para asegurar la inclusión de la identificación del cliente

en las transacciones tramitadas. Contar con información completa es fundamental para cumplir con los requisitos de la regulación así como para asegurar un monitoreo adecuado de las transacciones. Unas medidas adecuadas de control interno pueden incluir lo siguiente:

. • Mantener un sistema integral que identifique, para la totalidad del banco, las cuentas del libro mayor utilizadas como cuentas de concentración, así como los departamentos y personas autorizadas para usar esas cuentas.
. • Requerir dos firmas en los tiquetes del libro mayor.
. • Prohibir acceso directo de los clientes a las cuentas de concentración.
. • Capturar las transacciones de los clientes en los extractos de cuenta de los mismos.
. • Prohibir que los clientes conozcan las cuentas de concentración o que puedan impartir instrucciones a los empleados para que éstos realicen transacciones a través de esas cuentas.
. • Retener identificación adecuada sobre las transacciones y los clientes.
. • Frecuentemente asignar a una persona no relacionada con las transacciones para conciliar las cuentas.
. • Establecer un proceso oportuno para solucionar discrepancias.
. • Identificar los nombres de los clientes recurrentes.

Visión general ampliada – Actividades de préstamo

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las actividades de préstamo, y la capacidad de la gerencia para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Las actividades de préstamo incluyen, sin limitarse únicamente a ello, finca raíz, actividades de financiación comercial[127] y préstamos asegurados con efectivo, tarjetas de crédito, actividades comerciales y agrícolas. En las actividades de préstamo pueden intervenir muchas partes (por ejemplo, garantes, contratantes, mandantes o participantes en el préstamo).

FACTORES DE RIESGO

La intervención de muchas partes puede incrementar el riesgo de lavado de dinero o financiación del terrorismo cuando el origen y el uso de los fondos no son transparentes. Esta falta de transparencia puede generar oportunidades en cualquiera de las tres etapas de

las estratagemas de lavado de dinero o financiación del terrorismo. Estos planes pueden incluir lo siguiente:

. • Para lograr un préstamo, una persona adquiere un certificado de depósito con fondos ilícitos.
. • Los préstamos tienen un propósito ambiguo o ilegal.
. • Los préstamos se hacen o se pagan para un tercero.
. • El banco o el cliente procuran cortar o eliminar el rastro documental entre el prestatario y los fondos ilícitos.
. • Se otorgan préstamos personas que residen fuera de los Estados Unidos, especialmente en jurisdicciones y zonas geográficas de alto riesgo. Los préstamos también pueden incluir garantías ubicadas por fuera de los Estados Unidos.

FORMAS DE MITIGAR EL RIESGO

Todos los préstamos se consideran cuentas para los fines regulatorios del Programa de identificación del cliente (CIP por sus siglas en inglés). Para los préstamos que implican mayor riesgo de lavado de dinero y financiación del terrorismo, incluyendo los préstamos enumerados arriba, el banco debe realizar la debida diligencia de las partes relacionadas con la cuenta (por ejemplo, garantes, contratantes o mandantes). Realizar una debida diligencia adicional a que se requiere para una actividad de préstamo

[127] Consulte la sección de visión general ampliada titulada "Actividades de financiación comercial" en la página 140.

particular dependerá de los riesgos de la Ley de Secreto Bancario y Lavado de Dinero (BSA/AML), pero puede incluir verificación de referencias, obtener referencias de crédito, verificar el origen de las garantías y obtener extractos de los estados financieros o de la declaración de renta del prestatario así como de todas o varias de las personas que participan en el préstamo.

Los bancos deben contar con políticas, procedimientos y procesos para monitorear, identificar y reportar actividades inusuales o sospechosas. La sofisticación de los sistemas empleados para vigilar las cuentas de préstamos debe corresponder al tamaño y complejidad del negocio de préstamos de cada banco. Por ejemplo, los bancos pueden revisar los informes de préstamos, tales como pagos anticipados de préstamos, cuentas morosas, fraude o préstamos con garantía de efectivo.

Visión general ampliada – Actividades de financiación comercial

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las actividades de financiación comercial, y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Las actividades de financiación comercial típicamente comprenden financiación a corto plazo para facilitar la importación y exportación de bienes. Estas operaciones pueden incluir la transmisión de fondos para habilitar la transacción (por ejemplo, una carta de crédito), o por el contrario tratarse únicamente del pago de los fondos si no se cumplen los términos comerciales de las transacciones (por ejemplo, garantías independientes o cartas de crédito contingentes[♦] [standby letters of credit]). En ambos casos la participación del banco en las actividades de financiación comercial mitiga el riesgo para importadores y exportadores. La naturaleza de las actividades de financiación comercial requiere participación activa de múltiples partes en los dos lados de la transacción. Además de la relación básica exportador/importador que está al centro de toda actividad particular de comercio, puede haber relaciones entre exportadores y proveedores y entre importadores y clientes. Tanto el exportador como el importador pueden tener otras relaciones bancarias. Además, muchas otras entidades intermediarias financieras y no financieras pueden proporcionar servicios y conductos para agilizar los documentos subyacentes y los flujos de pagos asociados con las transacciones comerciales.

A manera de ejemplo, en un acuerdo de carta de crédito el banco puede servir como banco emisor y permitirle a su cliente (el comprador) adquirir bienes a nivel nacional o internacional, o puede actuar como banco asesor y permitirle a su cliente (el exportador) vender sus artículos a nivel nacional o internacional. La relación entre los dos bancos puede variar y en algunos casos puede ser similar a la de una relación corresponsal.

FACTORES DE RIESGO

La participación de múltiples partes puede hacer más difícil el proceso de la debida diligencia. Como tal, el banco debe realizar una revisión minuciosa y conocer completamente toda la documentación de la financiación comercial y los valores relacionados. Como el negocio de la financiación comercial puede depender más de

[♦] *Nota del Traductor*: Además de carta de crédito contingente / garantía independiente (Glosario para la empresa – terminología contable, tributaria y de administración, de Sylvana Debonis, Ed. La Ley, Buenos Aires, 2002, p. 180), otras definiciones para **standby letter of credit** son cartas de declaración de garantía (Diccionario de términos económicos, financieros y comerciales de E. Alcaraz y B. Hughes, Ed. Ariel, Barcelona, 1997, 2ª edición, p. 633) y letra de crédito disponible (Diccionario de banca de Jerry M. Rosenberg [trad. por Héctor Tejera], Ed. Ventura, México, 1997, p. 364-365).

documentos que otras operaciones bancarias, se presta para la falsificación de documentos, lo cual puede estar relacionado con el lavado de dinero, la financiación del terrorismo o con intentos por evitar sanciones de la OFAC u otras prohibiciones. Los bancos deben estar alertas a las transacciones de bienes de mayor riesgo (por ejemplo, comercio de armas o equipos nucleares).

Además, los bienes pueden estar sobrevalorados o subvalorados para evadir la reglamentación sobre el lavado de dinero (AML) o aduanera. Por ejemplo, un importador

puede pagar una alta suma con dineros provenientes de actividades ilícitas para adquirir bienes que básicamente carecen de valor y eventualmente son desechados. Los documentos comerciales tales como las facturas se adulteran para ocultar el esquema. Los fondos ilegales transferidos en la transacción comercial luego se emplean para comprar activos costosos tales como joyas, obras de arte, carros lujosos, aviones o embarcaciones, que pueden ser exportados a cualquier país.

Los bancos emisores mantienen relaciones de banca corresponsal extranjera para facilitar el comercio internacional. Los bancos deben cumplir las sanciones de la OFAC asegurándose de que las transacciones cuenten con licencia apropiada de la OFAC antes de la colocación de los fondos.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben practicar suficiente debida diligencia a todo cliente potencial de importación y exportación antes de abrir una cuenta o establecer una relación de crédito. Esta debida diligencia debe comprender una recopilación de información de los mandantes y beneficiarios, según sea adecuado, incluyendo su identidad, naturaleza de la empresa del cliente y el origen de su fortuna y fondos. Con respecto a las cartas de crédito, el banco asesor o el de confirmación pueden tener una relación de banco corresponsal con el banco emisor para facilitar el comercio, debido a la frecuencia de las transacciones en que ambas partes intervienen. O también podría tratarse de una transacción de una sola ocasión y el banco no tendría una relación formal con el banco emisor.

Las políticas, procedimientos y procesos deben requerir una revisión minuciosa de toda la documentación aplicable a la actividad de financiación, de manera que el banco pueda monitorear y reportar actividades inusuales o sospechosas. La sofisticación de los sistemas de informes y de información de gestión debe corresponder al tamaño y complejidad de las actividades de financiación comercial. Además de vigilar las transacciones financieras y los filtros de la OFAC, la revisión del banco debe detectar lo siguiente:

- Envíos de artículos que no corresponden al negocio que tiene el cliente.
- Clientes que negocian con jurisdicciones calificadas como de alto riesgo.
- Clientes que realizan transacciones con empresas que participan en actividades de mayor riesgo (por ejemplo, distribuidores de armas, materiales nucleares o sustancias químicas).
- Artículos que ingresan o salen de puertos de países no cooperantes.
- Fijación irregular de precios a los artículos.
- Cartas de crédito excesivamente enmendadas.
- Transacciones diseñadas para evadir las restricciones legales del país de origen.

Con respecto a la vigilancia de la asignación irregular de precios para los artículos, el examinador debe verificar que el banco revisa la documentación de las transacciones para determinar si en términos generales los precios concuerdan con los precios del mercado. Los empleados del banco que participan en la revisión de precios deben conocer los precios del mercado en términos generales.

Visión general ampliada – Banca privada

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las actividades de banca privada, y la capacidad de la gerencia para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes. Esta sección amplía la revisión fundamental de los requerimientos estatutarios y regulatorios de la banca privada, con el fin de proporcionar una evaluación más amplia de los riesgos de lavado de dinero (AML) asociados a esta actividad.

VISIÓN GENERAL

Las actividades de la banca privada se definen generalmente como aquellas en que se proporcionan servicios personalizados a clientes de alto valor neto (por ejemplo, planeación del patrimonio, asesoría financiera, préstamos, administración de inversiones, pago de cuentas, remisión de correo y mantenimiento de una residencia). La banca privada se ha convertido en una línea de negocio cada vez más importante para las organizaciones bancarias grandes y diversas, así como una fuente mejorada de ingresos por honorarios.

Los bancos de EE. UU. pueden administrar las relaciones de banca privada de clientes nacionales así como internacionales. Típicamente los umbrales de servicio de banca privada se basan en el número de activos que se administran y en la necesidad que exista de productos o servicios (por ejemplo, administración de finca raíz, supervisión de empresas cerradas, administración de dinero). Los honorarios que se cobran normalmente dependen del umbral de los activos y el uso de productos y servicios específicos.

Las organizaciones de banca privada típicamente se estructuran con un punto de contacto centralizado (por ejemplo, el gerente de relaciones), quien sirve den enlace entre el cliente y el banco y facilita la utilización por el cliente de los servicios y productos financieros del banco. El Apéndice N ("Banca privada – Estructura común") brinda 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 característicos de la relación de banca privada incluyen lo siguiente:

- Administración de dinero efectivo (por ejemplo, cuentas corrientes, privilegio de sobregiros, barridos de efectivo [cash sweeps] y servicios de pago de cuentas).
- Transferencia de fondos
- Administración de activos (por ejemplo, fideicomisos, asesoría de inversiones, administración de inversiones y servicios de custodia e intermediación).[128]
- Facilitación de entidades extraterritoriales [offshore entities] (por ejemplo, Sociedades de inversión privada (PIC por sus siglas en inglés), corporaciones de negocios internacionales (IBC por sus siglas en inglés) y fideicomisos).[129]

. • Servicios de préstamos (por ejemplo, hipotecarios, de tarjetas de crédito, préstamos personales, cartas de crédito).
. • Servicios de planeación financiera incluyendo planeación tributaria y patrimonial [estate planning].
. • Servicios de custodia.
. • Otros servicios según se requieran (por ejemplo, servicios de correo).

[128] Consulte la sección de procedimientos ampliados en "Servicios de administración de fideicomisos y activos" en la página 255.

La privacidad y confidencialidad son elementos importantes en las relaciones de banca privada. Aunque los clientes pueden usar los servicios de banca privada simplemente para manejar sus activos, también pueden buscar un refugio confidencial, seguro y legítimo para su capital. Cuando actúan como fiduciarias, los bancos tienen obligaciones estatutarias, contractuales y éticas que mantener.

FACTORES DE RIESGO

Los servicios de banca privada pueden prestarse para estratagemas de lavado de dinero y los procesos judiciales por lavado de dinero han demostrado esa susceptibilidad. El Subcomité Permanente de Investigaciones "Banca privada y lavado de dinero: estudio de caso sobre oportunidades y susceptibilidades",[130] describió parcialmente las siguientes susceptibilidades al lavado de dinero:

. • Los banqueros privados como promotores y defensores de los clientes.
• Clientes poderosos que incluyen personas expuestas políticamente, industriales y actores.
• Una cultura de confidencialidad y la utilización de jurisdicciones secretas o empresas ficticias.[131]
. • Una cultura de banca privada con controles internos laxos.
. • La naturaleza competitiva de la empresa.
. • Significativo potencial de utilidades para el banco.

Riesgo de las empresas ficticias [shell corporations]

Las empresas ficticias o de fachada existen en el papel pero no llevan a cabo prácticamente ningún negocio. Típicamente se emplean para realizar inversiones legítimas y pueden constituirse en los Estados Unidos (por ejemplo, en Delaware) o extraterritorialmente como IBC. Los riesgos que implican las empresas ficticias incluyen pocos registros de datos o incluso ninguno (por ejemplo, documentación sobre la propiedad), supervisión gubernamental inadecuada, carencia de divulgaciones

Consulte la sección de procedimientos ampliados en "Entidades corporativas (nacionales y extranjeras)" de la página 269.

[130] Consulte en: http://frwebgate.access.gpo.gov/cgi-

bin/getdoc.cgi?dbname=106_senate_hearing&docid=f:61699.wais.

[131] Una sociedad ficticia o de fachada [shell corporation] es una sociedad que no tiene presencia física en ningún país.

públicas y el gran rango de actividades autorizadas que pueden realizar en la jurisdicción de su constitución. Algunas sociedades ficticias emiten acciones al portador. Debido al alto grado de riesgo de lavado de dinero y financiación del terrorismo que tienen las acciones al portador, los bancos deben controlar las acciones al portador o encargarlas a terceros independientes confiables. Debido a que muchas sociedades ficticias permiten que las personas se amparen en la identidad jurídica de la sociedad, la debida diligencia puede resultar difícil.

FORMAS DE MITIGAR EL RIESGO

Contar con políticas, procedimientos y procesos eficaces ayuda a los bancos a no convertirse en medios o victimas del lavado de dinero, la financiación del terrorismo y otros delitos financieros que se comenten a través de las relaciones de banca privada. La sección de visión general fundamental titulada "Programa de debida diligencia de la banca privada (personas de ciudadanía no estadounidense)" de la página 75 contiene información adicional sobre la evaluación de riesgo y la debida diligencia. Si la supervisión gerencial es laxa, en última instancia, las actividades ilícitas realizadas a través de la unidad de banca privada pueden ocasionar costos financieros altos y generar riesgos para la reputación del banco. El impacto financiero puede incluir sanciones y multas regulatorias, gastos ocasionados por litigios, pérdidas en el negocio, reducción de liquidez, incautación y congelamiento de activos, pérdida de préstamos y gastos de reparaciones.

Evaluación del riesgo del cliente

Los bancos deben evaluar el riesgo que implican sus actividades de banca privada según el alcance de sus operaciones y la complejidad de sus relaciones con los clientes. La gerencia debe establecer un perfil de riesgo de cada cliente, que servirá para fijar prioridades en los recursos de supervisión y para el monitoreo continuo de las actividades de la relación. Se deben tomar en cuenta los siguientes factores al identificar las características del riesgo del los clientes de la banca privada:

. • Naturaleza del cliente y de su negocio. El origen de la riqueza del cliente, la naturaleza de su negocio y el grado hasta el cual los antecedentes del negocio del cliente representan un riesgo alto de lavado de dinero y financiación del terrorismo. Estos factores deben tomarse en cuenta para las cuentas de banca privada abiertas por personas expuestas políticamente.[132]

. • Propósito y actividad. El tamaño, propósito, tipos de cuentas, productos y servicios involucrados en la relación, y la actividad para la cual se abrió la cuenta.

. • Relación. La naturaleza y duración de la relación del banco (incluyendo las relaciones con los afiliados) con el cliente de banca privada.

. • Estructura del negocio del cliente. Tipo de estructura del negocio (por

ejemplo, IBC, sociedades ficticias (nacionales o internacionales) o PIC).

. • Localización y jurisdicción. Domicilio del cliente de banca privada y de su negocio (nacional o internacional). La revisión debe tomar en cuenta hasta

[132] Consulte la sección de visión general fundamental titulada "Programa de debida diligencia de la banca privada (para quienes no son ciudadanos de EE. UU.)" en la página 75 y la sección de visión general ampliada titulada "Personas políticamente expuestas" en la página 153.

dónde la respectiva jurisdicción está reconocida internacionalmente por presentar un riesgo mayor de lavado de dinero o, por el contrario, como una que tiene fuertes estándares de lucha contra el lavado de dinero.

- Información pública. Información conocida por el banco o razonablemente disponible al mismo sobre el cliente de banca privada. El alcance y la profundidad de esta revisión deben depender de la naturaleza de la relación y los riesgos involucrados.

Debida diligencia del cliente

La debida diligencia del cliente (CDD) es fundamental para establecer cualquier relación con un cliente, y es vital para los clientes de banca privada.[133] Los bancos deben adoptar medidas razonables para establecer la identidad de sus clientes de banca privada y si es adecuado, de los beneficiarios de las cuentas. La debida diligencia adecuada variará según los factores de riesgo identificados previamente. Las políticas, procedimientos y procesos deben definir la debida diligencia del cliente que es aceptable para los distintos tipos de productos (por ejemplo, PIC) servicios y cuenta habientes.

Los bancos deben verificar la información del cliente de las cuentas de banca privada mediante el Programa de identificación del cliente (CIP); sin embargo, este requerimiento mínimo no cubre a los beneficiarios de dichas cuentas. Para propósitos del CIP, no se requiere que un banco revise las cuentas de las personas jurídicas (por ejemplo, cuentas de banca privada abiertas para una PIC) para verificar la identidad de los beneficiarios. En cambio, solo se requiere que el banco verifique la identidad del cuenta habiente designado. No obstante, es posible que el banco deba tomar medidas adicionales para verificar la identidad de un cliente que no es persona natural (por ejemplo, una PIC), obteniendo para ello información sobre quienes poseen o detentan el control de la cuenta para verificar la identidad del cliente[134] y determinar si la cuenta se mantiene para personas que no son de ciudadanía estadounidense.[135]

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

. • El propósito de la cuenta.
. • El tipo de productos y servicios que se usarán.
. • Actividades previstas para la cuenta.
. • Descripción y antecedentes del origen de la riqueza del cliente.
. • El valor estimado neto de la riqueza del cliente, incluyendo los estados financieros.

. • El origen actual de los fondos de la cuenta.

[133]

Las políticas, procedimientos y procesos de debida diligencia son obligatorios para las cuentas de banca privada de personas que no son de ciudadanía estadounidense según la sección 312 de la Ley Patriota. Consulte la sección de visión general fundamental titulada “Programa de debida diligencia de banca privada (personas que no son de ciudadanía estadounidense)” en la página 75.

[134] Ver 31 CFR 103.121(b)(2)(ii)(C)

[135]

Ver “Programa de debida diligencia de banca privada para personas que no son de ciudadanía estadounidense)”, procedimientos fundamentales, en la página 202.

• Referencias u otra información para confirmar la reputación del cliente.

Supervisión por parte de la junta directiva y el personal directivo

La supervisión activa de la junta directiva y el personal directivo de banca privada y la creación de una cultura adecuada de supervisión corporativa son elementos fundamentales en una sólida gestión de riesgo y entorno de control. El propósito y los objetivos de las actividades de banca privada de la organización deben ser claramente identificados y comunicados por la junta y el personal directivo. Unas metas y objetivos bien desarrollados deben describir la base de clientes objetivo en términos de patrimonio neto mínimo, activos para inversión [investable assets] y tipos de productos y servicios buscados. Las metas y los objetivos deben también describir específicamente los tipos de clientes que el banco acepta y no acepta y fijar niveles de autorización adecuados para la aceptación de nuevos clientes. La junta y el personal directivo deben también participar activamente en el establecimiento de las metas de control y gestión de riesgo de las actividades de banca privada, incluyendo revisiones de auditoría y cumplimiento eficaces. Cada banco debe verificar que sus políticas, procedimientos y procesos para las actividades de banca privada sean evaluadas y actualizadas regularmente, y asegurarse de que las funciones, responsabilidades y obligaciones estén claramente delineadas.

Los planes de compensación de los empleados con frecuencia dependen del número de cuentas nuevas abiertas o incremento en los activos administrados. La junta y el personal directivo deben asegurarse de que los planes de compensación no generen incentivos para que los empleados ignoren la debida diligencia y los procedimientos adecuados de apertura de cuentas o las posibles operaciones sospechosas relacionadas con la cuenta. Los procedimientos que requieren autorización a varios niveles para aprobar cuentas nuevas de banca privada pueden minimizar estas oportunidades.

Debido al carácter delicado de la banca privada y el pasivo que potencialmente representa, los bancos deben investigar cuidadosamente los antecedentes de los gerentes de relaciones recién contratados y establecer un monitoreo continuo de su estado financiero personal, para detectar cualquier indicio de actividades inadecuadas. Sin embargo, cuando los gerentes de relaciones de banca privada cambian de empleadores, sus clientes con frecuencia se trasladan con ellos. Los bancos asumen la misma responsabilidad con los

clientes de los funcionarios recién contratados que asumen con cualquier nueva relación de banca privada. Por lo tanto esas cuentas deben ser revisadas oportunamente con los procedimientos del banco para nuevas relaciones de cuenta.

Los sistemas y reportes de información de gestión (MIS para Management Information Systems) son importantes también para la supervisión y administración eficaz de las relaciones y los riesgos de la banca privada. La junta y el personal directivo deben revisar los informes sobre la compensación del gerente de relaciones, el presupuesto o informes comparativos de objetivos así como informes aplicables de gestión de riesgo. Los reportes de información de gestión (MIS) de banca privada deben permitirle al gerente de relaciones supervisar y administrar integralmente a los clientes así como las relaciones asociadas a los mismos.

Visión general ampliada – Servicios de administración de fiducias y activos

OBJETIVO

Evaluar si las políticas, procedimientos, procesos y sistemas del banco son adecuados para manejar los riesgos asociados a los servicios de administración de fiducias y activos[136], y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Las cuentas de fiducia[137] [trust accounts] generalmente se definen como un convenio jurídico en el cual una parte (el fideicomitente o fiduciante [trustor / grantor]) transfiere la propiedad de los activos a una persona o banco (el fiduciario [trustee]) para tenerlos en depósito o utilizarlos en beneficio de terceros. Estos convenios incluyen amplias categorías de cuentas supervisadas por tribunales (por ejemplo, albaceazgo o custodias [executorship / guardianship]), fiducias personales (por ejemplo, fideicomisos activos [living trusts], fiducias establecidas por testamento y el fideicomiso benéfico), y los fideicomisos de sociedades (por ejemplo, administración fiduciaria de bonos).

En contraste con los convenios 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 agenciadas incluyen los servicios de administración en custodia de títulos, depósito fiduciario (garantía) [escrow], inversión[138] y las relaciones de custodia [safekeeping relationships]. Los productos y servicios de la agencia pueden ofrecerse en un departamento tradicional de fiducia o a través de otros departamentos del banco.

PROGRAMA DE IDENTIFICACIÓN DEL CLIENTE

Las reglas del Programa de identificación del cliente (CIP por sus siglas en inglés), vigentes desde el primero de octubre de 2003, aplican básicamente a todas las cuentas

[136] Las cuentas de administración de activos pueden ser cuentas de fiducias o de agencias administradas por el banco.

[137]

La OCC [Oficina del Contralor de la Moneda] y la OTS [Oficina de Supervisión de Entidades de Ahorro y Crédito] utilizan el término más amplio "capacidad fiduciaria" en vez de "fiducia". En la capacidad fiduciaria intervienen un fiduciario [trustee], un albacea testamentario, un administrador, un registrador de acciones y bonos, un agente de transferencia, un depositario [guardian], cesionario, receptor o un tutor [custodian] bajo la Ley de Donaciones Uniformes a Menores [Uniform Gifts to Minors Act]; [y] un asesor de inversiones, si el banco recibe honorarios por su asesoría de inversiones; cualquier capacidad bajo la cual el banco posee discreción para decidir en nombre de otro (12 CFR 9-2(e) y 12 CFR 550.30).

[138]

Para los propósitos de los bancos nacionales y las asociaciones reguladas por la OTS [Oficina de Supervisión de Entidades de Ahorro y Crédito], ciertas actividades de administración de inversiones, tales como proporcionar asesoría de inversión a cambio de honorarios, son "fiduciarias" por naturaleza.

de banco abiertas después de esa fecha. La regla CIP define que una "cuenta" incluye relaciones de administración de efectivo, de custodia [safekeeping], de tutoría [custodian] y fiducia. Sin embargo, la regla CIP excluye las cuentas de prestaciones sociales de empleados [employee benefit accounts] establecidas conforme a la Ley de Seguridad del Ingreso del Pensionado de 1974 (ERISA en inglés, para Employee Retirement Income Security Act).

Para los fines del CIP no es necesario que el banco investigue las fiducias, depósitos en garantía o cuentas similares para verificar la identidad de los beneficiarios, sino únicamente la identidad del cuenta habiente designado (la fiducia o el fideicomiso). En el caso de las cuentas de fiducia, el cliente es la fiducia, así el banco sea o no sea el fiduciario [trustee] en la fiducia. No obstante la regla del CIP también estipula que, con base en la evaluación realizada por el banco del riesgo que implica una cuenta nueva abierta por un cliente que no es persona natural, es posible que el banco deba "obtener información acerca" de las personas que tienen el control o la autoridad sobre la cuenta, incluyendo a los signatarios (firmantes), con el fin de verificar la identidad del cliente.[139] Por ejemplo, en ciertas circunstancias relativas a fiducias revocables [revocable trusts], es posible que el banco deba recopilar información sobre el fideicomitente [settlor], poderdante [grandor], fiduciario [trustee] u otras personas con autoridad para instruir al fiduciario, y que por lo tanto ejercen autoridad o control sobre la cuenta, con el fin de establecer la verdadera identidad del cliente.

En el caso de las cuentas de depósito en garantía [escrow accounts], si un banco abre una cuenta a nombre de un tercero --como por ejemplo un agente de finca raíz--quien actúa como agente de depósito en garantía, entonces el cliente del banco es el agente de depósito en garantía. Si el banco es el agente de depósito en garantía, entonces la persona que establece la cuenta es el cliente del banco. Por ejemplo, si un comprador de finca raíz abre directamente una cuenta de depósito en garantía y deposita fondos para pagarle al vendedor una vez satisfechas ciertas condiciones especificadas, el cliente del banco será el

comprador. Además, si una compañía en formación establece una cuenta de depósito en garantía 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 personería jurídica, la persona que abre la cuenta en su nombre). Sin embargo, la regla del CIP también estipula que, con base en la evaluación de riesgo hecha por el banco de una nueva cuenta abierta por un cliente que no es persona natural, es posible que el banco deba "obtener información acerca" de las personas que tienen autoridad o control sobre dicha cuenta, incluyendo a los signatarios, con el fin de verificar la identidad del cliente.[140]

FACTORES DE RIESGO

Las cuentas de administración de fiducias y activos, así como las relaciones con agencias, presentan riesgos relativos a la Ley del Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML) similares a los que tienen el recibo de depósitos, los préstamos y otras actividades bancarias tradicionales. Los problemas se deben

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

[140] Id [*Nota del Traductor*: Ibid.]

- Cuentas personales y cuentas supervisadas por tribunales.
- Cuentas de fiducia generadas en el departamento de banca privada.
- Cuentas de administración de activos y asesoría de inversiones.
- Cuentas nacionales y mundiales de custodia.
- Préstamos para títulos valores.
- Cuentas de prestaciones sociales de empleados y pensionados.
- Cuentas de fiducias corporativas.
- Cuentas de agentes de tranferencia.
- Otras líneas de negocio relacionadas.[141]

Como en cualquier otra relación de cuenta, el riesgo de lavado de dinero puede presentarse en los servicios de administración de fiducias y activos. Cuando hay uso indebido de las cuentas de administración de fiducias y activos se puede ocultar el origen y el uso de los fondos, así como la identidad de los titulares usufructuarios [beneficial owners] y propietarios legales. Los clientes y usufructuarios de las cuentas pueden tratar de permanecer anónimos con el fin de mover fondos ilícitos o evitar investigaciones. Por ejemplo, los clientes pueden buscar cierto nivel de anonimato creando Sociedades de inversión privada (PIC), fiducias extraterritoriales [offshore trusts] u otras entidades de inversión que ocultan la propiedad real o el derecho de usufructo de la fiducia.

FORMAS DE MITIGAR EL RIESGO

La gerencia debe fijar políticas, procedimientos y trámites que le permitan al banco identificar relaciones y circunstancias de cuentas inusuales, activos y origen de activos

cuestionables y otras áreas potenciales de riesgo (por ejemplo, cuentas extraterritoriales, PIC, fiducias de protección de activos [APT, para asset protection trusts],[142] cuentas de agencias, y beneficiarios no identificados). Mientras que la mayoría de las administradoras de fiducias y activos tradicionales no necesitarán una debida diligencia mejorada, la gerencia debe estar alerta respecto a las situaciones que requieren revisión o investigación adicional.

Comparación de los clientes con los listados

El banco debe tener la capacidad de mantener la información del CIP y realizar la verificación, efectuada únicamente una vez, de los nombres de las cuentas de fiducia contra las solicitudes de búsqueda según la sección 314(a). El banco también debe poder identificar a los clientes que puedan estar expuestos políticamente (PEP), que negocian o se localizan en las jurisdicciones designadas como "de preocupación especial en cuanto al lavado de dinero" bajo la sección 311 de la Ley Patriota, o que concuerdan con las listas de la OFAC.[143] Como buena práctica, el banco también debe determinar la identidad de las demás partes que puedan controlar la cuenta, tales como los fiduciantes [grantors] o fiduciarios asociados [co-trustees].

Consultar los manuales apropiados de cada agencia bancaria federal para conocer las definiciones específicas de estos productos.

[142] Las fiducias de protección de activos (APT en inglés) son una forma especial de fiducia irrevocable, por lo general creada (liquidada) extraterritorialmente con el fin principal de preservar y proteger una parte de la riqueza de una persona contra los acreedores. El título 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 suplir a los beneficiarios.

Consulte la sección de visión general fundamental titulada "Información compartida" como guía adicional sobre los procedimientos para compartir información; para la solicitud de investigación 314(a), consulte la página 55 y la sección de visión general ampliada titulada "Personas expuestas políticamente" para obtener más información, en la página 153.

Circunstancias que garantizan una debida diligencia mejorada

La gerencia debe evaluar el riesgo de una cuenta con base en diferentes factores, que pueden incluir los siguientes:

- El tipo de cuenta de fiducia o agencia y su tamaño.
- Los tipos y frecuencia de las transacciones.
- El país de residencia de los titulares o beneficiarios, o el país en el que se establecieron, u origen de los fondos.
- Las cuentas y las transacciones que no son usuales o acostumbradas para el cliente o el banco.

Deben establecerse procedimientos estrictos de documentación, verificación y monitoreo de

transacciones para las cuentas que la gerencia considere de alto riesgo. Típicamente las cuentas de las prestaciones sociales de los empleados y las cuentas supervisadas por tribunales están entre las de más bajo riesgo para la Ley de Secreto Bancario y Lucha contra el Lavado de Dinero (BSA/AML).

A continuación se presentan ejemplos de situaciones en las cuales puede ser apropiado realizar la debida diligencia mejorada:

- El banco está iniciando una relación con un cliente.
- Los titulares o beneficiarios de la cuenta residen en una jurisdicción extranjera, o la fiducia o sus mecanismos de fondos están establecidos extraterritorialmente.
- Los activos o las transacciones son inusuales para el tipo y carácter del cliente.
- El tipo, tamaño, activos o transacciones de la cuenta son inusuales para el banco.
- Las transferencias de fondos internacionales se realizan particularmente a través de fuentes de fondos extraterritoriales.
- Las cuentas se financian con activos fácilmente trasladables, tales como piedras preciosas, metales preciosos, monedas, obras de arte, estampillas excepcionales o instrumentos negociables.

[143] La gerencia y los examinadores deben saber que la concordancia con las listas de la OFAC no es un requerimiento de la Ley de Secreto Bancario (BSA). Sin embargo, dado que los sistemas de fiducia típicamente son distintos a los sistemas bancarios y están separados de los mismos, la verificación de estos chequeos en el sistema bancario no basta para asegurar que los mismos también se lleven a cabo en el departamento de administración de fiducias y activos.

- Se mantienen cuentas o relaciones en las que la identidad de los titulares o usufructuarios o el origen 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.[144]
- Interés en cuentas de fiducia de abogados (IOLTA [interest on lawyers' trust accounts]) que tienen y tramitan montos significativos en dólares.
- Los activos de las cuentas incluyen PIC.
- En las cuentas o transacciones son parte algunas personas políticamente expuestas (PEP).

Consulte la sección de visión general ampliada titulada "Organizaciones no gubernamentales y entidades de beneficencia" en la página 162, para mayor orientación.

Visión general ampliada – Extranjeros no residentes y personas naturales extranjeras

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las transacciones de cuentas de extranjeros no residentes (NRA [nonresident aliens]), y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Los extranjeros que mantienen relaciones con los bancos de EE. UU. pueden dividirse en dos categorías: extranjeros residentes y extranjeros no residentes. Como definición, un extranjero no residente es una persona que no es ciudadana de los EE. UU. y: (i) no es residente permanente legal de Estados Unidos durante el año calendario y no cumple con la prueba de presencia física,[145] o (ii) no le ha sido emitida una tarjeta de recibo de registro como extranjero, también conocida como tarjeta verde [green card]. El Servicio de Ingresos Nacionales [Internal Revenue Service] determina las responsabilidades tributarias del extranjero y oficialmente lo define como "residente" o "no residente".

Aunque los extranjeros no residentes no son residentes permanentes, tienen una necesidad válida de establecer una relación de cuenta con un banco de Estados Unidos. Los extranjeros no residentes usan los productos y servicios del banco para resguardar activos (por ejemplo, para mitigar pérdidas debidas a [fluctuaciones en] la tasa de cambio), expansión de negocios e inversiones. El monto de los depósitos de extranjeros no residentes colocado en el sistema bancario de EE. UU. se ha calculado entre cientos de miles de millones de dólares [hundreds of billions] y aproximadamente un billón de dólares [$1 trillion][◆]. Aún en el extremo bajo del rango, la magnitud es significativa, tanto en términos del sistema bancario de los EE.UU como en términos económicos.

[145] Un ciudadano extranjero [foreign nacional] es un extranjero con permiso de residencia [resident alien] si la persona está físicamente presente en los Estados Unidos durante al menos 31 días del año calendario actual y está presente 183 días o más según el siguiente conteo: todos los días en que estuvo presente durante el año actual, más un 1/3 de los días que estuvo presente durante el año anterior, más 1/6 de los días en el año anterior a ese. Algunos días de presencia no cuentan, tales como (i) los días transcurridos en Estados Unidos debido una enfermedad que haya evolucionado durante la presencia del extranjero en Estados Unidos, impidiéndole irse, (ii) los días que los viajeros frecuentes [commuters: hacia y desde el trabajo y el hogar] se trasladan hacia o desde Canadá o México, (iii) un día de menos de 24 horas transcurrido en tránsito entre dos ciudades fuera de Estados Unidos, y (iv) los días en que el extranjero es persona exenta. La persona se considera extranjero residente para los fines de los impuestos federales e impuestos de empleo desde el primer día de su presencia física en Estados Unidos en el año que se cumple la prueba. Favor consultar el sitio de Internet del Servicio de Ingresos Nacionales [Internal Revenue Service] en www.irs.gov.

[◆] [*Nota del Traductor*: Es frecuente encontrar variaciones en la traducción de estas cifras elevadas; en este caso hemos usado la siguiente correspondencia: *one billion* como mil millones y *one trillion* como un billón (numéricamente, la cifra 10^{12} **en EE. UU**., puesto que en el Reino Unido puede significar 10^{18})].

Puede resultar más difícil para los bancos verificar y autenticar la identificación de un

cuenta habiente extranjero no residente, así como el origen de sus fondos y de su riqueza, y ello puede implicar riesgos con respecto a la Ley del Secreto Bancario y la Lucha contra el Lavado de Dinero (BSA/AML). El país de origen del extranjero no residente también puede aumentar el riesgo de la cuenta, dependiendo de las leyes de secreto [confidencialidad] que tenga ese país. Puesto que se espera que los extranjeros no residentes residan fuera de los Estados Unidos, las transferencias de fondos o el uso de cajeros automáticos extranjeros puede ser más frecuente. El riesgo BSA/AML puede ser mayor si el extranjero no residente es una persona expuesta políticamente (PEP). Consulte la sección de procedimientos ampliados titulada "Personas expuestas políticamente" en la página 259 para obtener más información.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben fijar políticas, procedimientos y trámites que permitan una debida diligencia y prácticas de verificación seguras, evaluación del riesgo de las cuentas de los extranjeros no residentes, y monitoreo y reporte de actividades inusuales o sospechosas. Los siguientes factores deben tomarse en cuenta al determinar el nivel de riesgo de una cuenta de un extranjero no residente:

- El país de origen del cuenta habiente.
- Los tipos de los productos y servicios utilizados.
- Tipos de identificación.
- El origen de la riqueza y los fondos.
- Actividades inusuales en la cuenta.

Los clientes extranjeros no residentes pueden solicitar la condición W-8 para que le practiquen retención de impuestos en Estados Unidos. En tales casos, el cliente no extranjero diligencia el formulario W-8, el cual certifica la condición de exención de impuestos en Estados Unidos y en el extranjero. Si bien este formulario W-8 es emitido por el Servicio de Ingresos Nacionales (IRS por sus siglas en ingles), no se envía al IRS; se archiva en el banco para sustentar la no retención de impuestos sobre las ganancias a dicho extranjero.[146]

El Programa de identificación del cliente (CIP) debe detallar los requisitos de identificación que deben cumplir los extranjeros no residentes para abrir una cuenta. El programa debe incluir métodos documentales y no documentales para verificar [la identidad de] los clientes. Además, la Ley Patriota enmendó la Ley del Secreto Bancario para requerir una debida diligencia especial para las cuentas de banca privada de personas extranjeras, incluyendo a las personas que están expuestas políticamente o a políticos extranjeros de alto nivel.

[146] Se puede encontrar información adicional sobre este tema en www.irs.gov/formspubs.

Visión general ampliada – Personas expuestas políticamente

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las transacciones realizadas por personas expuestas políticamente (PEP por sus siglas en inglés), y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Para los propósitos de este manual, una persona expuesta políticamente es alguien que durante los procedimientos normales de apertura, mantenimiento o cumplimiento de una cuenta es identificado como "político extranjero de alto nivel" o miembro de la "familia inmediata" de dicho político o "asociado cercano" del mismo.

La guía para las agencias [del gobierno de Estados Unidos] expedida en enero de 2001, brinda a los bancos recursos que pueden ayudarles a determinar si una persona es político extranjero de alto nivel o miembro de su familia inmediata o asociado cercano del mismo.[147] Según esta guía:

. • Un "político extranjero de alto nivel" es un alto funcionario de las ramas ejecutiva, legislativa, administrativa, militar o judicial de un gobierno extranjero (ya sea elegido o no), alto funcionario de un importante partido político extranjero o alto ejecutivo de una empresa de un gobierno extranjero. Además, el concepto de político extranjero de alto nivel incluye a cualquier corporación, empresa u otra entidad creada por dicho funcionario o para su beneficio.

. • La "familia inmediata" del político extranjero de alto nivel típicamente incluye a los padres, hermanos, cónyuge, hijos o parientes políticos.

. • Un "asociado cercano" de un político extranjero de alto nivel es una persona ampliamente conocida públicamente como alguien que tiene una relación inusualmente estrecha con un político extranjero de alto nivel, e incluye a quienes están en posición de realizar grandes transacciones financieras nacionales e internacionales en nombre del político extranjero de alto nivel. Si bien es más difícil para los bancos identificar a los asociados cercanos, éstos incluyen a personas cuya relación con la PEP les permite realizar grandes transacciones financieras nacionales e internacionales en nombre de la PEP.

FACTORES DE RIESGO

"Guía para la investigación detallada de las transacciones que puedan incluir fondos derivados de instancias de corrupción oficial extranjera" emitida por el Tesoro de los EE.UU, la Junta de Gobernadores de

Sistema de la Reserva Federal, la Corporación Federal de Seguros de Depósitos, la Oficina del Contralor de la Moneda, la Oficina de Supervisión de Entidades de Ahorro y Crédito, y el Departamento de Estado, enero de 2001.

En los últimos años, en los casos de alto perfil, las PEP han utilizado los bancos como conducto para sus actividades ilícitas, las que incluyen corrupción, soborno y lavado de dinero. Los bancos que negocian con PEP que son deshonestas ponen en juego su reputación y se exponen a investigaciones detalladas así como a medidas de supervisión.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben obtener información integral mediante una debida diligencia practicada a las PEP y fijar políticas, procedimientos y procesos que permitan una investigación y vigilancia más detalladas de todas las cuentas de las PEP. Los procedimientos de apertura de cuenta son fundamentales porque representan la oportunidad más favorable para el banco de recopilar la siguiente información sobre las PEP:

- Identidad del cuenta habiente y del usufructuario de la misma.
- Origen de los fondos.
- Origen de la riqueza.
- Información sobre los miembros de la familia inmediata o asociados cercanos que están autorizados para efectuar transacciones en la cuenta.
- Objetivo de la cuenta, volumen esperado y naturaleza de la actividad de la cuenta.

Las cuentas de las PEP no existen únicamente en los bancos grandes o internacionales. Una PEP puede abrir una cuenta en cualquier banco, sin tomar en cuenta su tamaño o localización. Los bancos deben identificar específicamente las cuentas de las PEP y evaluar el grado de riesgo involucrado, el cual variará. La alta gerencia debe participar en la decisión de aceptar una cuenta de una PEP. Si la gerencia encuentra que una cuenta ya abierta pertenece a una PEP, se deben evaluar los riesgos y adoptar medidas apropiadas. El monitoreo continuo de las cuentas de PEP es fundamental para asegurar que el uso dado a las cuentas sea el previsto. La Ley de Secreto Bancario (BSA) requiere practicar la debida diligencia a las cuentas de banca privada de algunas PEP.[148]

[148] Consulte la sección de visión general fundamental titulada: "Programa de debida diligencia de banca privada (personas no estadounidenses)", en la página 75.

Visión general ampliada – Cuentas de embajadas y consulados extranjeros

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las

transacciones realizadas en cuentas de embajadas y consulados extranjeros, y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Las embajadas comprenden las oficinas del embajador extranjero, el representante diplomático, y su gabinete. La embajada, dirigida por el embajador, es la representación oficial de un gobierno extranjero en los Estados Unidos (u otro país). Las oficinas de los consulados extranjeros se desempeñan como sucursales de la embajada y cumplen distintas diferentes funciones administrativas y gubernamentales (por ejemplo, emitir visas y encargarse de la inmigración). Los consulados extranjeros típicamente se localizan en zonas metropolitanas principales. Además, los representantes diplomáticos de los embajadores extranjeros y sus familias y asociados pueden ser considerados como personas expuestas políticamente (PEP) en ciertas circunstancias.[149]

Las embajadas y consulados extranjeros en Estados Unidos deben acceder al sistema bancario para cumplir con muchas de sus obligaciones financieras cotidianas. Tales servicios pueden ir desde relaciones de cuentas para gastos operacionales (por ejemplo, nómina, arriendos y servicios) hasta transacciones inter e intra-gubernamentales (por ejemplo, compras comerciales y militares). Además de las cuentas oficiales de la embajada, algunos bancos prestan u ofrecen servicios o cuentas auxiliares al personal de las embajadas y a sus familias, así como a funcionarios del gobierno extranjero actual o de gobiernos anteriores. Cada una de estas relaciones representa diferentes niveles de riesgo para el banco.

Las cuentas de las embajadas, incluyendo las cuentas de oficinas específicas de las embajadas tales como las de un ministerio de cultura o educación, agregado militar o ministerio de defensa, o cualquier otra cuenta, deben tener un propósito operativo específico que indique la función oficial de la oficina del gobierno extranjero. Conforme a las prácticas establecidas para las relaciones comerciales, estas cuentas de embajadas deben contar con una autorización escrita del gobierno extranjero.

FACTORES DE RIESGO

Para poder prestar servicios a embajadas y consulados, es posible que los bancos de EE. UU. deban mantener relación de corresponsalía con el banco de la embajada o consulado extranjero. Los bancos que efectúan negocios con embajadas o consulados

Consulte la sección de visión general ampliada titulada “Personas expuestas políticamente” en la página 153 para obtener información adicional.

. • Las cuentas son de países que han sido calificados como de alto riesgo.
. • Se hacen grandes transacciones de dinero en las cuentas.

. • La actividad de la cuenta no se realiza conforme al propósito de la misma (por ejemplo, valija bancaria [transporte de moneda o instrumentos financieros pouch activity] o pagadera mediante identificación adecuada).
. • Las cuentas financian directamente los gastos personales de extranjeros, incluyendo, sin limitarse únicamente a ello, los gastos de los estudiantes universitarios.
. • Los negocios oficiales de la embajada se realizan a través de las cuentas personales.

FORMAS DE MITIGAR EL RIESGO

Los bancos deben obtener información a partir de la debida diligencia integral practicada a las relaciones de cuenta de embajadas y consulados. Concretamente para las cuentas de banca privada de personas no estadounidenses, deben obtener la información de debida diligencia que pide 31 CFR 103.181.[150] La debida diligencia del banco practicada a las relaciones de cuenta de embajadas y consulados debe corresponder a los niveles de riesgo respectivos. Además, se espera que los bancos fijen políticas, procedimientos y procesos que permitan un examen y vigilancia más detalladas de todas las relaciones de cuenta de embajadas y consulados extranjeros. La gerencia debe conocer plenamente la finalidad de las cuentas y el volumen y naturaleza de las actividades previstas de las mismas. La vigilancia permanente de las relaciones de cuenta de embajadas y consulados extranjeros es fundamental para asegurar el uso previsto de las mismas.

[150] Consulte la sección de visión general fundamental titulada “Programa de debida diligencia de la banca privada (personas no estadounidenses)” en la página 75 para recibir orientación adicional.

Visión general ampliada – Entidades financieras no bancarias

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las cuentas de entidades financieras no bancarias (NBFI por sus siglas en inglés), y la capacidad gerencial para implementar sistemas eficaces de monitoreo y elaboración de informes.

VISIÓN GENERAL

Las NBFI se definen en términos generales como entidades que prestan servicios financieros. La Ley Patriota define una variedad de entidades como entidades financieras.[151] Los ejemplos más frecuentes de entidades financieras no bancarias (NBFI) son los siguientes, sin limitarse únicamente a ellos:

. • Casinos y clubes de juego.
. • Compañías de títulos valores y productos básicos (por ejemplo, agencias e intermediarios, asesores de inversión, fondos mutuos, fondos de cobertura o comerciantes de productos básicos).
. • Empresas de servicios de dinero (por ejemplo, ciertas empresas que cambian cheques por efectivo, establecimientos que negocian dinero o casas de cambio; emisores o vendedores de cheques viajeros o giros postales y tarjetas de valor acumulado [stored value cards] o quienes los redimen [redeemers]; empresas que trasladan dinero [transmitters].
. • Otras entidades financieras (por ejemplo, comerciantes de metales preciosos, piedras preciosas o joyas; casas de empeño; empresas de préstamos o financieras).

Algunas NBFI actualmente están obligadas a crear un programa de Lucha contra el Lavado de Dinero (AML), cumplir con los requisitos de registros de la Ley de Secreto Bancario (BSA) y reportar operaciones sospechosas, tal como aplica para los bancos. Las NBFI típicamente requieren una cuenta bancaria para poder operar. Si bien las NBFI mantienen cuentas operativas en bancos, la BSA no requiere y ni FinCEN ni las agencias bancarias federales esperan que los bancos acaben convirtiéndose en entidades reguladoras *de facto* de ninguna industria de NBFI o cliente alguno de las NBFI. Además, si bien se espera que los bancos manejen el riesgo que pueden presentar todas las cuentas, incluyendo las de las NBFI, los bancos no serán responsables del cumplimiento de los clientes de éstas con la BSA y otras leyes y regulaciones federales y estatales.

Guía para la prestación de servicios bancarios a negocios de servicios monetarios

[151] Consulte el Apéndice D: "Definición estatutaria de entidad financiera".

El 26 de abril de 2005 FinCEN y las agencias bancarias federales emitieron una guía interpretativa que aclara los requisitos de la BSA y las expectativas de supervisión que aplican a las cuentas abiertas para los negocios de servicios monetarios o que se mantienen para dichos negocios.[152] La guía consigna las siguientes expectativas mínimas de debida diligencia que deben seguir los bancos al abrir o mantener cuentas de empresas de servicios

monetarios:

. • Confirmar el registro ante FinCEN, si se requiere.
. • Confirmar la licencia del Estado [de EE. UU.] respectivo, si aplica.
. • Confirmar la categoría del agente, si aplica.
. • Realizar una evaluación de riesgo para determinar el nivel de riesgo asociado a cada cuenta y si se requiere extender la debida diligencia.

Mientras que varios componentes específicos de la guía son particulares a los negocios de servicios financieros (tales como la expectativa de confirmar el registro en FinCEN), el fundamento de la guía –que sostiene que los bancos deben aplicar los requerimientos de la BSA según la evaluación del riesgo– aplica a las cuentas de todos los clientes de las NBFI, según se describe en la sección de mitigación del riesgo que se presenta abajo.

FACTORES DE RIESGO

Las industrias NBFI son extremadamente diversas e incluyen desde grandes corporaciones multinacionales hasta pequeñas empresas independientes que ofrecen servicios financieros únicamente como un componente auxiliar en su negocio principal (por ejemplo, una tienda de abarrotes que también preste el servicio de cambio de cheques por dinero en efectivo). El rango de productos y servicios ofrecidos, y las bases de clientes servidos por las NBFI, son igualmente diversos.

Los bancos que tienen relaciones de cuenta con las NBFI pueden estar expuestos a mayor riesgo de lavado de dinero porque muchas NBFI presentan las siguientes características:

- No mantienen relaciones permanentes con sus clientes y no requieren ninguna o tan solo mínima identificación de los clientes.
. • Llevan registros limitados o inconsistentes sobre sus clientes y sus transacciones.
. • Frecuentemente realizan transacciones de dinero.
. • Están sujetas a niveles variables de requisitos regulatorios y de supervisión.
. • Pueden cambiar su combinación de productos o su localización con facilidad y rápidamente ingresar o terminar una operación.
. • Algunas veces operan sin el debido registro o licencia.

FORMAS DE MITIGAR EL RIESGO

Consulte en la: “Guía interpretativa para las diferentes agencias sobre la prestación de servicios bancarios a empresas de servicios monetarios que operan en los Estados Unidos”, disponible en www.fincen.gov.

. • Identificar las relaciones NBFI.
. • Evaluar los riesgos potenciales que presentan las relaciones NBFI.
. • Realizar una debida diligencia adecuada y continua a las relaciones NBFI cuando sea necesario.

. • Asegurarse de que las relaciones NBFI se tomen en cuenta debidamente en los sistemas del banco de monitoreo y reporte de actividades sospechosas.

Factores de evaluación de riesgo

Los bancos deben evaluar los riesgos que presentan sus clientes NBFI y dirigir sus recursos de la forma más adecuada hacia las cuentas que presentan mayor riesgo de lavado de dinero. Se pueden utilizar los siguientes factores para identificar los riesgos relativos del portafolio de las NBFI. No obstante, la gerencia debe sopesar y evaluar cada factor de evaluación de riesgo para producir una determinación de riesgo para cada cliente y establecer prioridades entre los recursos con que se cuenta para la supervisión. Entre los factores de riesgo relevantes están los siguientes:

. • Tipos de productos y servicios que ofrece la NBFI.
. • Localidades y mercados que atiende la NBFI.
. • Actividad prevista de la cuenta.
. • Propósito de la cuenta.

La debida diligencia de un banco debe corresponder al nivel de riesgo del cliente NBFI identificado a través de la evaluación del riesgo. Si la evaluación de riesgo de un banco indica mayor riesgo de lavado de dinero o financiación del terrorismo, se espera que amplíe la debida diligencia de manera acorde con el riesgo incrementado.

Visión general ampliada – Proveedores de servicios profesionales

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las relaciones con los proveedores de servicios profesionales, y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Los proveedores de servicios profesionales actúan como intermediarios entre sus clientes y los bancos, e incluyen a abogados, contadores, agentes de inversión y otros terceros que sirven de enlace financiero a sus clientes. Estos proveedores pueden realizar negocios financieros para sus clientes. Por ejemplo, un abogado puede prestarle servicios a un cliente o hacer arreglos para que éstos se presten en nombre del cliente, como por ejemplo cierre de transacciones de finca raíz, transferencia de activos, administración de los dineros del cliente, servicios de inversión y convenios de fiducia.

Un ejemplo típico es el interés que producen las llamadas “cuentas de fiducia de abogados” (IOLTA por sus siglas en inglés). Estas cuentas tienen fondos de distintos clientes de abogados [o de firmas de abogados] pero actúan como cuenta bancaria estándar con una

característica particular: el interés que produce la cuenta se cede a la asociación de abogados del Estado [de Estados Unidos] [state bar association] u otra entidad de interés público para fines de donación de trabajo [pro bono work -sin cobro de honorarios].

FACTORES DE RIESGO

En contraste con las cuentas de depósito en garantía que se establecen para servir a clientes individuales, las cuentas de proveedores de servicios profesionales permiten transacciones comerciales continuas con múltiples clientes. Generalmente el banco no tiene una relación directa con los titulares de estas cuentas, ni los conoce, y éstos pueden ser un grupo de personas naturales o jurídicas que cambian constantemente.

Como sucede con cualquier cuenta que presenta riesgo por terceros, el banco se expone a un mayor riesgo de la práctica ilegal de lavado de dinero. Algunos ejemplos potenciales de este tipo de práctica ilegal son:

. • Lavado de dineros ilícitos.
. • Estructuración de depósitos o retiros de dinero.
. • Apertura de cuenta para un tercero con el propósito principal de ocultar la identidad del cliente subyacente.

FORMAS DE MITIGAR EL RIESGO

Al establecer y mantener relaciones con proveedores de servicios profesionales, los bancos deben evaluar adecuadamente los riesgos de las cuentas y vigilar la relación para detectar operaciones sospechosas o inusuales. Cuando abre una cuenta el banco debe conocer el propósito de la misma, incluyendo el volumen previsto de transacciones, los productos y servicios utilizados y las localizaciones geográficas en donde se lleva a cabo la relación. Como se indica en la sección de visión general fundamental titulada “Exención del informe de transacciones en moneda” de la página 51, no es posible eximir a los proveedores de servicios profesionales de los requisitos que aplican al reporte de transacciones en moneda.

Visión general ampliada – Organizaciones no gubernamentales y entidades de beneficencia

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las cuentas de organizaciones no gubernamentales (ONG) y entidades de beneficencia, y la capacidad gerencial para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Las ONG son organizaciones sin ánimo de lucro que se dedican a actividades cuyo propósito es contribuir al bienestar público. Las ONG pueden prestar servicios sociales básicos, trabajar para aliviar el sufrimiento, promover los intereses de los pobres, informar a los gobiernos sobre los problemas de los ciudadanos, incentivar la participación política, proteger el medio ambiente o encargarse del desarrollo de la comunidad para atender las necesidades de los ciudadanos, organizaciones o grupos en una o más de las comunidades en que trabajan. Una ONG puede ser cualquier organización sin ánimo de lucro que sea independiente del Gobierno.

Las ONG pueden ser desde grandes entidades regionales o nacionales de beneficencia o grupos comunitarios de auto-ayuda [auto gestión]. También comprenden institutos de investigación, iglesias, asociaciones de profesionales y grupos de presión y cabildeo. Económicamente las ONG típicamente dependen parcial o totalmente de donaciones benéficas y del trabajo voluntario.

FACTORES DE RIESGO

Puesto que las ONG pueden usarse para obtener fondos para organizaciones de beneficencia, el flujo de fondos hacia las ONG así como desde éstas hacia fuera puede ser complejo y las torna susceptibles al abuso por parte de lavadores de dinero y terroristas. En consecuencia, las autoridades se han vuelto más rigurosas con respecto a las ONG.

FORMAS DE MITIGAR EL RIESGO

Para evaluar el riesgo de los clientes de las ONG los bancos deben practicarle una debida diligencia adecuada a la organización. Además de obtener la información del Programa de identificación del cliente (CIP), la debida diligencia debe centrarse en otros aspectos de la organización, como por ejemplo:

. • Propósito o ideología.
. • Las áreas geográficas atendidas (incluyendo la sede principal y las zonas en donde opera).
. • La estructura de la organización.
. • La base de donantes y voluntarios.
. • Criterios de financiación y desembolso (incluyendo la información básica del beneficiario).
. • Requisitos en cuanto a registros.
. • Afiliaciones con otras ONG, gobiernos o grupos.
. • Controles internos y auditorias.

Para las cuentas que la gerencia del banco considere de alto riesgo, se deben establecer procedimientos estrictos en cuanto a documentación, verificación y vigilancia de las transacciones. Las cuentas de ONG con mayor riesgo BSA/AML incluyen las que operan o prestan servicios a nivel internacional, realizan actividades inusuales o sospechosas o carecen de documentación adecuada. La debida diligencia mejorada de estas cuentas debe

incluir lo siguiente:

- Evaluación de los mandantes o titulares.
- Obtener y revisar los estados financieros y auditorias.
- Verificar el origen y la utilización de los fondos.
- Evaluar a los grandes contribuyentes y donantes de la ONG.
- Verificar las referencias.

Visión general ampliada – Corporaciones (nacionales y extranjeras)

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a las transacciones realizadas por corporaciones nacionales y extranjeras, y la capacidad de la gerencia para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

El término "corporaciones" incluye a distintos tipos de sociedades que pueden utilizarse para muchos fines, como por ejemplo la planeación tributaria y patrimonial. Es relativamente fácil constituir una corporación. Las personas naturales y asociaciones y sociedades, así como corporaciones ya constituidas, pueden constituir corporaciones legítimas, pero estas entidades [de todas maneras] se prestan para el lavado de dinero y la financiación del terrorismo.

Entidades corporativas nacionales

Las corporaciones ficticias [shell corporations] registradas en Estados Unidos constituyen un tipo de entidad corporativa nacional que puede presentar alto riesgo.[153] En algunas jurisdicciones de Estados de EE. UU. únicamente se requiere un mínimo de información para registrar los estatutos de constitución de una corporación y mantener el prestigio o buen nombre de la misma –todo lo cual incrementa la probabilidad de que las organizaciones delictivas y terroristas abusen de ellas–.

Entidades corporativas extranjeras

Las entidades corporativas extranjeras más frecuentemente utilizadas son las fiducias, los fondos de inversión y las empresas de seguros. Dos entidades extranjeras que pueden presentar mayor riesgo de lavado de dinero son las corporaciones de negocios internacionales (IBC por sus siglas en inglés) y las sociedades de inversión privada (PIC por sus siglas en inglés) abiertas en centros financieros extraterritoriales (OFC por sus

siglas en inglés).[154] Muchos OFC están sujetos a relativamente pocos requisitos en cuanto a divulgación pública [de información] y mantenimiento de registros cuando se establece una entidad corporativa extranjera, lo cual crea un entorno oportuno para el lavado de dinero.

[153] Una corporación ficticia o fantasma se define como una corporación que no tiene presencia física en ningún país.

[154] Si bien algunos OFC [centros financieros extraterritoriales] están bien regulados, la atracción principal del sector extraterritorial [offshore] siguen siendo los contextos jurídicos diseñados para ocultar la identidad de los titulares usufructuarios, promover el arbitraje regulatorio y de supervisión, y proporcionar formas de mitigar o evadir impuestos en el país de origen.

Las corporaciones de negocios internacionales (IBC) son entidades creadas en países distintos al de residencia de la persona, que pueden ser utilizadas para resguardar la confidencialidad u ocultar activos. Utilizarlas implica una serie de ventajas tales como las siguientes, sin limitarse únicamente a ellas:

- Proteger los activos.
- Planeación patrimonial.
- Privacidad y confidencialidad.
- Reducción de la carga tributaria.

A través de una IBC, una persona puede realizar las siguientes transacciones:

- Abrir y mantener cuentas bancarias.
- Mantener y transferir fondos.
- Hacer negocios internacionales y otras transacciones relacionadas.
- Mantener y manejar inversiones extraterritoriales (por ejemplo, en acciones, bonos, fondos mutuales y certificados de depósito), muchas de las cuales pueden no estar disponibles para las “personas” según su lugar de residencia.
- Tener tarjetas débito y crédito corporativas, y disponer así de acceso fácil a los fondos.

Sociedades de inversión privada (PIC)

Las PIC son entidades jurídicas independientes. Ofrecen confidencialidad en cuanto a la propiedad, tienen los activos centralizados y pueden servir de intermediarias entre clientes de banca privada y los potenciales beneficiarios de la PIC. Una PIC también puede ser una inversión de una cuenta de fiducia. Las PIC con frecuencia se constituyen en países que cobran impuestos bajos o no cobran impuestos sobre los activos y las operaciones empresariales o que son paraísos o refugios en cuanto al secreto bancario.

FACTORES DE RIESGO

Los riesgos de lavado de dinero y financiación del terrorismo se presentan porque las

entidades corporativas pueden ocultar la identidad de los verdaderos propietarios de los activos o propiedades derivadas de actividades delictivas o de una asociación con las mismas. La privacidad y confidencialidad que caracterizan a algunas entidades corporativas puede ser explotada por delincuentes, lavadores de dinero y terroristas. Verificar la identidad del fideicomitente o fiduciante [grantor] y usufructuario de algunas corporaciones puede ser extremadamente difícil, puesto que las características de estas entidades protegen la identidad legal de sus propietarios. Pocos registros públicos divulgan la identidad de los verdaderos propietarios. En general, la falta de transparencia en cuanto a la propiedad; los requerimientos mínimos o nulos en cuanto a los registros que se deben llevar, la divulgación de información financiera y la supervisión; y el rango de actividades permisibles –todo ello incrementa el riesgo de lavado de dinero–.
Aunque es posible constituir corporaciones en la mayoría de las jurisdicciones internacionales, la mayor parte de ellas se constituye en OFC [centros financieros extraterritoriales] que ofrecen privacidad e imponen pocas o ninguna obligación tributaria. Para mantener el anonimato, muchas entidades corporativas se constituyen con directores nominales, funcionarios nominales y accionistas nominales. En ciertas jurisdicciones es posible constituir corporaciones mediante acciones al portador [bearer shares]; no se mantienen registros de propiedad, y la propiedad se basa más bien en la posesión física de los certificados de las acciones. Las fiducias revocables son otra forma de aislar a los fideicomitentes o fiduciantes y usufructuarios y pueden ser designadas como propietarias y administradoras de la entidad corporativa, constituyendo una barrera significativa al cumplimiento de la ley.

Si bien las empresas ficticias ubicadas en los Estados Unidos han sido utilizadas con fines legítimos, también han sido objeto de abuso como conducto para el lavado de dinero y han ocultado transacciones realizadas en ultramar o la existencia de estructuras corporativas nacionales o extranjeras estratificadas [layered]. Se han detectado empresas ficticias registradas en los Estados Unidos que realizan transacciones sospechosas con contrapartes extranjeras. Estas transacciones consisten principalmente en transferencias circulares de fondos que ingresan y salen del sistema bancario estadounidense aparentemente sin propósito comercial alguno. Debe sospecharse especialmente de las entidades corporativas nacionales cuyos nombres son similares a los de los bancos y que carecen de autoridad regulatoria para realizar operaciones bancarias.

FORMAS DE MITIGAR EL RIESGO

La gerencia debe fijar políticas, procedimientos y procesos que le permitan al banco identificar las relaciones de cuenta, especialmente las cuentas depósito, y vigilar los riesgos asociados a estas cuentas en todos los departamentos del banco. Los clientes de las corporaciones pueden abrir cuentas en el departamento de banca privada, el departamento de fiducias o en sucursales locales. La gerencia debe establecer una debida diligencia mejorada en la apertura de la cuenta y durante la vida de la relación, para administrar el riesgo de estas cuentas. El banco debe recopilar suficiente información sobre las entidades corporativas y sus titulares usufructuarios para conocer y evaluar los riesgos de la relación de cuenta. Entre la información más importante para determinar el uso lícito de estas entidades está: el tipo de negocio, el propósito de la cuenta, el origen de los fondos y el

origen de la riqueza del usufructuario.

El Programa de identificación del cliente (CIP) del banco debe detallar los requisitos de identificación para la apertura de una cuenta de una sociedad corporativa. Al abrirle cuentas a clientes que no son personas naturales, según 31 CFR 103.121 los bancos pueden obtener información sobre las personas que ejercen autoridad y control sobre dichas cuentas para verificar la identidad de los clientes (siendo el cliente la sociedad corporativa). La información que se requiere para abrir una cuenta puede incluir los estatutos de constitución, una resolución corporativa adoptada por sus directores autorizando la apertura de la cuenta, o la designación de una persona para actuar como signataria de la entidad en la cuenta. Debe ponerse especial atención a los estatutos que permiten la existencia de accionistas y miembros de junta directiva nominales así como acciones al portador.
Si a través de los departamentos de fiducia y banca privada el banco le facilita a clientes nuevos o actuales la constitución de sociedades corporativas, el riesgo de lavado de dinero por lo general se reduce. Puesto que el banco conoce a las partes (por ejemplo, fideicomitentes, beneficiarios y accionistas) que conforman la entidad corporativa, la debida diligencia inicial y la verificación se facilitan. Además, en dichos casos, el banco con frecuencia tiene relaciones en curso con los clientes que están iniciando la constitución de una sociedad corporativa.

La evaluación del riesgo puede incluir una revisión de la jurisdicción nacional o internacional en donde se constituyó la entidad corporativa, el tipo de cuenta (o cuentas) y las actividades previstas comparadas con las actividades reales, el tipo de productos que se utilizarán y si la sociedad corporativa fue creada en el banco o externamente. Si la propiedad se detenta mediante acciones al portador, el banco debe conservar el control físico de las mismas ya sea en el mismo banco o a través de un tercero confiable, para asegurarse de que la propiedad de la corporación no cambie sin el conocimiento del banco. La evaluación efectuada por el banco del riesgo que implica una corporación se torna más compleja en las organizaciones corporativas complejas. Por ejemplo, una IBC extranjera puede constituir una serie estratificada de entidades corporativas, cada una de las cuales nombra a su entidad matriz como su beneficiaria.

Es necesario ejercer una vigilancia permanente de las cuentas para asegurarse que sean revisadas para detectar actividades inusuales o sospechosas. El banco debe estar alerta a las transacciones de alto riesgo efectuadas en esas cuentas, tales como actividades sin propósito comercial o legítimo aparente, transferencias de fondos desde y hacia jurisdicciones de alto riesgo, transacciones intensivas en moneda y cambios frecuentes en la propiedad o el control de las sociedades corporativas privadas.

Visión general ampliada – Negocios intensivos en capital [Cash Intensive Businesses]

OBJETIVO

Evaluar si los sistemas del banco son adecuados para manejar los riesgos asociados a los negocios intensivos en capital, y la capacidad de la gerencia para implementar sistemas eficaces de debida diligencia, monitoreo y elaboración de informes.

VISIÓN GENERAL

Los negocios y entidades intensivas en capital están presentes en distintos sectores de la industria. La mayoría de estos negocios realizan negocios lícitos; no obstante, algunos aspectos de estos negocios pueden ser susceptibles al lavado de dinero o a la financiación del terrorismo. Los ejemplos comunes incluyen, pero no se limitan, a los siguientes:

. • "Rapi-tiendas" [convenience stores].
. • Restaurantes.
. • Almacenes minoristas.
. • Licoreras.
. • Distribuidores de cigarrillos.
. • Cajeros automáticos de propiedad privada.
. • Operadores de máquinas de ventas [vending machines].
. • Parqueaderos.

FACTORES DE RIESGO

Algunos negocios y entidades pueden ser mal utilizados por los lavadores de dinero para legitimar sus ingresos ilícitos. Por ejemplo, un delincuente puede ser el propietario de un negocio intensivo en capital, como un restaurante, y usarlo para lavar dinero proveniente de actividades ilícitas. Los depósitos de dinero que hace el restaurante en su banco aparentemente no son nada inusual porque ese negocio legítimamente es generador de efectivo. Sin embargo, el volumen de dinero que maneja un restaurante que lava dinero probablemente es mayor en comparación con el de restaurantes similares en la zona. La naturaleza de los negocios intensivos en capital y la dificultad para identificar las actividades inusuales puede hacer que estos negocios se consideren de alto riesgo.

FORMAS DE MITIGAR EL RIESGO

Al establecer y mantener relaciones con negocios que son intensivos en capital, los bancos deben fijar políticas, procedimientos y procesos para identificar las relaciones de alto riesgo; evaluar el riesgo de lavado de dinero; realizar la debida diligencia durante la apertura de cuentas y periódicamente durante la relación; e incluir tales relaciones en el monitoreo adecuado de actividades inusuales y sospechosas. Al abrir una cuenta, los bancos deben conocer las operaciones que realiza el negocio del cliente; el propósito de la cuenta, incluyendo el volumen de transacciones previsto, los productos y servicios utilizados y la región geográfica donde se desarrolla la relación.

Cuando se lleva a cabo la evaluación de riesgo de negocios intensivos en capital, los bancos deben dirigir sus recursos hacia las cuentas que presenten el mayor riesgo de lavado de dinero y financiación del terrorismo. Los siguientes factores pueden usarse para identificar los riesgos:

. • Propósito de la cuenta.

. • Volumen, frecuencia y naturaleza de las transacciones de dinero.
. • Antecedentes del cliente (por ejemplo, duración de la relación, Informes de transacciones monetarias (CTR) radicados,[155] Informes de operaciones sospechosas (ROS) radicados).
. • Actividad principal del negocio, productos y servicios ofrecidos.
. • Estructura de la corporación o el negocio.
. • Localización geográfica y jurisdicciones donde se realizan las operaciones.
. • Disponibilidad de información y cooperación del negocio para suministrar información.

Para aquellos clientes considerados como de alto riesgo, la gerencia del banco puede pensar en implementar prácticas sólidas, como visitas periódicas a la sede del negocio, entrevistas con la gerencia del negocio, o revisiones detalladas de las transacciones.

. • Estructura de la corporación o el negocio.
. • Localización geográfica y jurisdicciones donde se realizan las operaciones.
. • Disponibilidad de información y cooperación del negocio para suministrar información.

Para los clientes considerados de alto riesgo, la gerencia del banco puede pensar en implementar prácticas sólidas, como visitas periódicas a la sede del negocio, entrevistas con la gerencia del negocio o revisiones detalladas de las transacciones.

[155] Como se describe en la sección de visión general fundamental titulada “Exenciones del informe de transacciones monetarias” en la página 51, algunas entidades no califican para las exenciones de dicho informe de transacciones monetarias como negocios que no cotizan en la bolsa.