¿Por qué soy responsable por el cumplimiento en mi empresa?

Debido a que usted vende giro postales o realiza envíos de dinero, está sujeto a los requisitos de cumplimiento de varias leyes contra el lavado de dinero y sobre prevención del fraude, así como a otras reglamentaciones de cumplimiento relacionadas, como las siguientes:

- **Ley de Secreto Bancario (Bank Secrecy Act, BSA)**
- **Ley PATRIOTA de los EE. UU. (USA Patriot Act)**
- **Ley Dodd–Frank de Protección al Consumidor y Reforma de Wall Street (Dodd–Frank Wall Street Reform and Consumer Protection Act)**
- **Ley Gramm–Leach–Bliley (Gramm–Leach–Bliley Act)**
- **Oficina de Control de Activos Extranjeros (Office of Foreign Assets Control, OFAC)** y otras listas de sanciones

Ley de Secreto Bancario (BSA)

Exige que las instituciones financieras estadounidenses ayuden a los organismos gubernamentales estadounidenses a detectar y prevenir el lavado de dinero. Específicamente, la ley exige que las instituciones financieras mantengan registros de las compras en efectivo de instrumentos negociables, presenten informes de transacciones en efectivo que superen los $10,000 (monto total diario) e informen actividades sospechosas que podrían implicar lavado de dinero, evasión impositiva u otra actividad delictiva. Fue aprobada por el Congreso de los Estados Unidos en 1970.

Ley PATRIOTA de los EE. UU.

El Título III de la Ley PATRIOTA de los EE. UU. tiene como objetivo facilitar la prevención del lavado de dinero internacional y la financiación del terrorismo, la detección de estos y las acciones judiciales contra ellos. Los artículos del título principalmente modifican partes de la Ley de Control de Lavado de Dinero de 1986 y la Ley de Secreto Bancario de 1970.

Las disposiciones del Título III se dividen en tres subtítulos. El primero aborda principalmente el fortalecimiento de las normas bancarias específicas contra el lavado de dinero, en especial, en la esfera internacional. La comunicación entre las fuerzas de orden público y las instituciones financieras, así como entre instituciones, se expande a través del segundo subtítulo, que también incrementa los requisitos de mantenimiento de registros y presentación de informes. La parte final del título aborda el contrabando de divisas y la falsificación de dinero, incluida la cuadruplicación de la sanción máxima para la falsificación de moneda extranjera.

Ley Dodd–Frank de Protección al Consumidor y Reforma de Wall Street

Esta ley exige que la Oficina de protección financiera al consumidor emita nuevas normas para proteger a los consumidores que envían dinero por vía electrónica a otros países. Todas las personas que realizan envíos de dinero, así como los bancos, las instituciones de ahorro o las cooperativas de crédito que ofrecen transferencias internacionales en el curso normal de sus actividades comerciales, deben cumplir con las nuevas normas. Las normas afectan a todas las transferencias efectuadas por un cliente en los Estados Unidos y enviadas a otro país. La ley fue promulgada el 21 de julio de 2010.

Usted tiene responsabilidades específicas y exigidas como agente de MoneyGram conforme a esta ley. Revise estos requisitos con regularidad en la Sección 10, Ley Dodd–Frank, de esta carpeta de recursos.

Ley Gramm–Leach–Bliley

Esta ley exige que la Comisión federal de comercio (Federal Trade Commission, FTC) emita una norma de salvaguarda definitiva para establecer los estándares relacionados con las salvaguardas de información administrativa, técnica y física a fin de que las instituciones financieras garanticen la seguridad y la confidencialidad de los registros y la información del cliente, ofrezcan protección contra cualquier amenaza o riesgo previstos con relación a la seguridad y a la integridad de esos registros, y protejan contra el acceso o uso no autorizados de los registros o la información que podría resultar en un daño importante o inconveniente para cualquier cliente.

Las responsabilidades adicionales como agente de MoneyGram según esta ley se detallan en mayor detalle en la ***página 18*** de esta guía de recursos.

Su programa de cumplimiento <u>debe</u> alinearse con los requisitos de estas y otras reglamentaciones gubernamentales como se describe en este Recurso de cumplimiento.

Oficina de Control de Activos Extranjeros (OFAC)

La OFAC es una división del Departamento del Tesoro de los EE. UU. y es responsable de aplicar los programas de sanciones del gobierno de los EE. UU. a países, organizaciones e individuos. Los programas de sanciones, por lo general, implican el bloqueo de activos para favorecer la seguridad nacional. Muchas de las personas sancionadas, comúnmente conocidas como ciudadanos especialmente designados (Specially Designated Nationals, SDN), son narcotraficantes y terroristas conocidos o se sospecha que lo son. Se prohíbe a todas las entidades de los EE. UU. realizar cualquier transacción financiera con los SDN, incluso si dichas transacciones se originan o se completan fuera de los Estados Unidos.

Como compañía de los EE. UU., MoneyGram debe cumplir con las sanciones de los EE. UU. con relación a Cuba. Ni MoneyGram ni sus agentes pueden procesar transacciones en las que el remitente o el beneficiario sea ciudadano cubano. Dichos temas DEBEN remitirse al Departamento de cumplimiento de AML de MoneyGram llamando al **1-800-444-3010**.

Para obtener más información sobre la OFAC, visite el sitio web del Departamento del Tesoro en:

www.ustreas.gov/offices/enforcement/ofac.

El sitio también incluye una extensa lista de preguntas y respuestas habituales sobre la OFAC.

Mensaje Código 4 de posible coincidencia

MoneyGram revisa *todos* los nombres de los remitentes y beneficiarios de envíos de dinero y los compara con *diversas* listas de sanciones, incluida la lista de SDN de la OFAC, *independientemente* del monto en dólares de la transacción. Si un nombre es una posible coincidencia con la lista de sanciones monitoreada, los agentes deben seguir las instrucciones de MoneyGram a fin de evitar cualquier pago o reembolso no autorizado.

Si recibe un mensaje de **Código 4** sobre un intento de transacción, debe seguir los siguientes pasos:

1. Se le indicará que se comunique con MoneyGram al **1-800-444-3010** y seleccione la **Opción 2** ANTES de completar transacciones individuales o múltiples.
2. Debe comunicarse con MoneyGram *antes* de rechazar O completar la transacción.
3. El representante de MoneyGram solicitará información adicional para verificar que el nombre del cliente realmente coincida con la lista de sanciones.

¡Su colaboración es fundamental!

NO se pueden pagar ni reembolsar las transacciones hasta que MoneyGram haya revisado y divulgado las posibles coincidencias con los SDN de la OFAC.

Sanciones civiles y penales

El gobierno puede imponer sanciones civiles y penales severas a toda persona que viole la BSA, la Ley PATRIOTA de los EE. UU., la OFAC, la Ley Dodd–Frank u otras leyes y reglamentaciones contra el lavado de dinero y el fraude. Las multas civiles y penales pueden alcanzar rápidamente cientos de miles o, incluso, millones de dólares. La sanción penal por violar el requisito de la BSA es una multa de hasta $500,000, una pena de prisión de hasta 10 años, o ambas. Además, el gobierno podría incautar los bienes involucrados en violaciones penales de estas leyes. Esto incluye su empresa, su cuenta bancaria o cualquier otro bien que el gobierno pueda relacionar con la actividad criminal.

En determinadas ocasiones, se les puede imputar a las empresas los actos cometidos por sus empleados. Es importante que sus empleados se capaciten sobre estos temas y que su empresa cuente con un sistema adecuado para asegurarse de que los empleados cumplan con las leyes y las reglamentaciones. Si usted o sus empleados no lo hacen, podrá estar sujeto a grandes multas y/o a una pena de prisión.

El gobierno exige el cumplimiento estricto de estas leyes y reglamentaciones.

MoneyGram cancelará de inmediato el contrato de cualquier agente que, con conocimiento o por negligencia, no cumpla con las leyes y las reglamentaciones.

No vale la pena arriesgarse a no cumplir.

¿Qué es el lavado de dinero?

El lavado de dinero es el intento de ocultar o de disfrazar la naturaleza, la localidad, la fuente, la propiedad o el control del dinero obtenido en forma ilegítima.

Esta definición cubre una amplia variedad de actividades y no se limita a las transacciones con dinero en efectivo o divisas. El lavado de dinero puede incluir cualquier tipo de dinero, por ejemplo, giro postales, envíos de dinero y otras transacciones financieras. Es necesario comprender cómo se lava el dinero para poder identificar y denunciar la actividad y también saber cómo ayudar a evitar que ocurra.

El ciclo del lavado de dinero comienza cuando los delincuentes colocan dinero en el sistema financiero, a través de, por ejemplo, la compra de giro postales o del envío de dinero. Una vez que el dinero haya ingresado a los sistemas financieros, se disfraza aún más el origen de los fondos ilegítimos mediante la transferencia a través de diversas instituciones financieras, tales como cuentas bancarias o de inversión. Por último, el dinero ingresa a la economía diaria y parece ser legítimo mediante la compra de artículos o la inversión legítima, como por ejemplo, bienes raíces, propiedades inmuebles, acciones y bonos, o mediante la compra de giro postales adicionales o el envío de dinero adicional.

Actividad terrorista y lavado de dinero

En la mayoría de los casos, el lavado de dinero se relaciona con el tráfico de drogas y la evasión de impuestos. Sin embargo, muchas veces, los ***terroristas*** intentan lavar dinero con la intención de ocultar su identidad y financiar sus operaciones ilegales. Es fundamental que cualquier persona que procese transacciones relacionadas con dinero, como las de MoneyGram, permanezca alerta a dichas actividades y, si se detectan, tome las medidas adecuadas de inmediato.

El **Grupo de Acción Financiera (Financial Action Task Force, FATF)** y la **Red de Control de Delitos Financieros (Financial Crime Enforcement Network, FinCEN) del Tesoro de los EE. UU.** han proporcionado orientación sobre las transacciones financieras que podrían ser indicio de financiación terrorista en los sitios web www.fatf-gafi.org y www.fincen.gov.

Algunos ejemplos incluyen, *a título enunciativo, lo siguiente:*

- Movimiento de fondos a través de un país que la FinCEN o el FATF designaron como país “no colaborador”, individuos identificados como ciudadanos especialmente designados por la OFAC, o que aparecen en la lista de cuentas bloqueadas de las Naciones Unidas.
- Múltiples transacciones realizadas por un grupo de ciudadanos de países asociados con actividades terroristas.
- Personas que representan a otro negocio que transmite dinero y que utiliza MoneyGram para transferir fondos a diversas localidades. Esto puede ser indicio de entidades de transferencia de dinero sin licencia que desean evitar el uso del sistema bancario para realizar envíos de dinero en moneda extranjera.

Si sospecha que existe financiación terrorista, debe denunciar el incidente de inmediato a la línea directa de la FinCEN al 1-800-556-3974, que funciona las 24 horas, los siete (7) días de la semana. También debe presentar en forma electrónica un **Informe de actividad sospechosa (SAR, consulte a continuación)** sobre cualquier actividad terrorista que sospeche.

Para ayudar a prevenir el lavado de dinero en efectivo y obtener documentación que se pueda utilizar para entablar una acción judicial contra las personas que se dedican al lavado de dinero, el gobierno exige que guarde y almacene registros sobre determinadas transacciones con dinero en efectivo. Para algunas transacciones, también se deben guardar y presentar informes en forma electrónica. Consulte las páginas 14 a 16 de la Sección 1 y las Secciones 7 y 8 de esta carpeta de recursos para obtener información adicional sobre la presentación electrónica de estos tipos de informes.

¿Qué es el fraude?

El fraude es el robo potencial o real de información y fondos de usted como agente y de los clientes a través del *engaño, de la trampa, de la falsificación o de la manipulación* u otros medios *ilícitos*.

¡Esté atento!
Existen tres áreas críticas de fraude que los agentes de MoneyGram deben reconocer y colaborar para prevenir mediante el monitoreo de transacciones diarias:

- **Fraude contra el agente.**
- **Fraude de falsificación.**
- **Fraude contra el cliente.**

Fraude contra el agente

Los agentes y sus empleados a menudo son víctimas de personas que intentan robar información del agente o del cliente para cometer fraude. Por lo general, estos intentos se agrupan en una de las siguientes categorías, entre otras: ***delitos informáticos o ingeniería social (phishing).*** *Consulte el* ***Recurso rápido para el mostrador para la prevención de fraude****, que se encuentra en el bolsillo de esta carpeta de recursos, para obtener información adicional sobre estos tipos de fraude contra el agente.*

Si sigue las pautas a continuación, podrá prevenir muchos de estos intentos hacia sus empleados y su empresa:

- No comparta información confidencial con NADIE.
- Instale y conserve un software de detección y eliminación en tiempo real de virus, spyware y malware.
- Cierre la sesión o apague los equipos cuando no estén en uso.
- No revise el correo electrónico, acceda a Internet ni use la banca electrónica en la computadora en la que procesa transacciones de envío y recepción de dinero de MoneyGram.
- No responda correos electrónicos; no abra archivos adjuntos ni haga clic en enlaces de correos electrónicos de CUALQUIER remitente que no conozca al utilizar cualquier computadora.
- Dese cuenta de que es posible que los mensajes emergentes que declaran que su equipo está infectado y ofrecen software para escanear o solucionar el problema no sean legítimos. Confirme con un experto antes de hacer clic en un mensaje emergente. De ser posible, cancele.
- **Nunca envíe una transacción de “prueba” o “capacitación”. NUNCA.**
- **Nunca** envíe una transacción sin tener el dinero en efectivo en mano y un cliente en persona en la localidad.
- No intente comenzar ninguna transacción que se inicie por teléfono.
- Elimine o restrinja las funciones de contestación de llamadas en su teléfono comercial.
- *Evalúe regularmente a sus empleados sobre estas pautas y capacítelos sobre las técnicas ilegítimas.*

Proteja su PIN

- No comparta su PIN con NADIE.
- Cambie el PIN cada vez que un empleado deje la empresa.
- Cambie el PIN periódicamente.
- NUNCA declare su PIN o número de agente delante de un cliente.
- No publique ni escriba su PIN en un lugar en el que el cliente pueda verlo.
- No proporcione su PIN por teléfono a menos que usted inicie la llamada a MoneyGram.

Fraude de falsificación de instrumentos financieros y giro postales

Cuando las impresoras láser a color computarizadas comenzaron a hacer copias en alta resolución, apareció un nuevo tipo de alteración fraudulenta o falsificación de dinero. Estas fácilmente pueden imprimir documentos cuya calidad es difícil de distinguir de los documentos reales. Estos documentos incluyen, a título enunciativo, *cheques comerciales/personales, dinero en efectivo, cheques de viajeros* y *giro postales falsos.*

Utilice la siguiente guía para evitar las transacciones fraudulentas con giro postales:

Cuando venda giro postales

- Cobre el efectivo de la compra de giro postales **ANTES** de imprimir y entregarlos alcliente.
- Confirme que el efectivo cobrado no contenga billetes falsos.
  Visite www.secretservice.gov/money_detect.shtml para obtener más ayuda sobre cómo detectar billetes falsos.

Cuando cobre giro postales

- La banda de advertencia en la parte superior del giro postal presentará características de seguridad que debe confirmar antes de intentar cobrarlos.
- Verifique que el giro postal no tenga alteraciones. Mire de cerca el monto del valor en dólares, la fecha, el beneficiario y el comprador para asegurarse de que ninguno de estos datos se haya modificado.
- Verifique si el giro postal tiene partes borradas o manchas pequeñas, decoloración o cualquier daño.
- Solicite al cliente que endose el giro postal con el nombre exactamente como aparece en el frente del giro postal.
- Obtenga la misma identificación que para el cobro de cheques.

Llame a MoneyGram INMEDIATAMENTE al 1-800-542-3590 si tiene alguna duda sobre un giro postal, para confirmar el monto en dólares o detener el estado de pago. También puede visitar www.moneygram.com y hacer clic en el enlace **Giro postal** en **“Products and Services”** (Productos y servicios).

RECUERDE

MoneyGram NUNCA llamará a los agentes para solicitarles que procesen envíos de dinero de cualquier tipo ni que procesen un giro postal por CUALQUIER motivo.

Fraude contra el cliente

MoneyGram se esfuerza todos los días para evitar que los clientes se conviertan en víctimas del fraude. MoneyGram está comprometido con su capacitación para que usted pueda educar a sus clientes y así crear una red de envío de dinero más segura y más confiable. ***La clave es conversar y no, confrontar.***

Al impedir que se completen transacciones fraudulentas, se protegerá a usted, a nuestros clientes y a la marca global MoneyGram. El fraude puede ocurrir durante transacciones de **envío Y recepción**. Abajo encontrará una guía sobre algunos de los tipos más comunes de estafas fraudulentas contra el cliente e instrucciones sobre cómo investigar más antes de completar las transacciones.

Familiar en necesidad:

A menudo, la “estafa del familiar en necesidad” comienza con una llamada telefónica del estafador que se hace pasar por un ser querido o incluso un agente de las fuerzas policiales o un abogado, para solicitarle dinero a fin de ayudar con la atención médica, la reparación de un automóvil, el pago de una fianza, etc. **Si sospecha que procesa una transacción para alguien que es víctima de esta estafa, haga algunas preguntas simples, en tono de conversación, como las siguientes:**

¿Qué está haciendo su familiar en (nombre del lugar)? ¿Es común que esté ahí?

¿Ha enviado dinero a (nombre del beneficiario) o utilizado alguna vez MoneyGram? ¿Por qué motivos?

¿Ha confirmado con otros familiares que el beneficiario está en otro país?

Loterías o concursos:

Una víctima de la “estafa de la lotería o concurso” es posible que envíe dinero a una empresa u organización en lugar de a una sola persona. Por lo general, recibieron la notificación de que “ganaron” por correo electrónico o correo postal, de modo que preste atención a las copias impresas de correos electrónicos o a un sobre que contenga la carta a la que hace referencia el remitente mientras completa el formulario. **Haga preguntas como:**

Nunca escuché acerca de la lotería u organización que llevó adelante este concurso, ¿cómo se enteró usted?

Nunca escuché que alguien tuviera que enviar dinero para cubrir impuestos o tarifas de aduana, ¿sabe por qué le solicitaron que lo haga?

Compra en línea:

El envío de dinero para una compra en línea ***siempre debe ponerlo en alerta***. La mayoría de los sitios de Internet ofrecen una opción de pago diferente que brinda un mejor nivel de protección para el comprador y el vendedor que el envío de dinero. Si alguien desea pagar un artículo en línea, considere lo siguiente:

¿Utiliza una pregunta y respuesta de prueba en relación con el artículo? Es una advertencia definida de que algo puede no ser legítimo.

¿Mencionó que envía dinero para pagar un servicio o un artículo comprado a través de Internet?

A menudo, lo enviará dentro de los Estados Unidos.

Romance:

En muchos casos, el cliente dice que conoció a alguien o que alguien los contactó en línea y cree ser parte de una relación “romántica”. Aprovechándose del estado emocional del cliente, el estafador le pedirá que envíe dinero para que pueda visitarlo o mudarse para empezar una vida juntos. No debe dudar de hacer averiguaciones sobre su interés romántico mediante preguntas, y recuerde sugerencias como:

¿Hace cuánto que conoce a (el beneficiario)?

¿Cómo se conocieron?

¿Analizó planes de viaje alternativos donde usted no fuera el que tiene que pagar?

¿Cuál es la urgencia?

¿Está enviando a otro país, como Nigeria, Jamaica o Canadá?

Otros tipos de estafas fraudulentas contra el cliente incluyen, entre otros, los siguientes:

- Estafa con cheques o giro postales.
- Estafa de zona de desastre.
- Estafa de compra de vehículo.
- Estafa de préstamo falso.
- Estafa de anuncio en el periódico.
- Estafa del comprador misterioso.

Para obtener más información sobre estos y otros tipos de actividades fraudulentas, visite regularmente el sitio www.moneygram-preventfraud.com

Si sospecha que se trata de una transacción fraudulenta, incluso si tiene dudas al respecto, informe DE INMEDIATO a MoneyGram por teléfono al 1-800-866-8800 o por correo electrónico a fraudalert@moneygram.com.

Red de control de delitos financieros (FinCEN)

La Red de control de delitos financieros (Financial Crimes Enforcement Network, FinCEN) es una agencia dentro del Departamento del Tesoro de los EE. UU. que administra las leyes y las reglamentaciones contra el lavado de dinero del gobierno federal. La FinCEN ha creado materiales para colaborar con los Negocios de Servicios Monetarios (siglas en Inglés MSB) en el cumplimento de estas leyes y reglamentaciones.

Los MSB deben familiarizarse con la información que proporciona la FinCEN y deben revisar regularmente el sitio web de la FinCEN dedicado a los MSB, www.fincen.gov. (seleccione *Information for Money Services Businesses* [Información para negocios de servicios monetarios]) para obtener actualizaciones o nueva información relacionada con el cumplimiento de las normas contra el lavado de dinero.

A continuación se detalla parte de la información disponible en el sitio web de la FinCEN*:

Página de inicio de MSB: Esta sección proporciona información importante sobre los MSB, que incluye información sobre la inscripción del MSB, materiales sobre los MSB en inglés y en siete idiomas extranjeros, y contactos adicionales, como los contactos pertinentes de los estados. También proporciona noticias recientes para los MSB.

Guía: Esta sección tiene como finalidad clarificar cuestiones o responder a preguntas generales sobre las reglamentaciones de la FinCEN que se aplican a los MSB.

Presentación electrónica: Esta sección contiene instrucciones y enlaces para la presentación electrónica.

Avisos/comunicados/hojas informativas: Esta sección contiene avisos de la FinCEN sobre el lavado de dinero y otros delitos financieros. También contiene comunicados de utilidad y hojas informativas para los MSB.

Enlaces rápidos: Existen enlaces rápidos a información general sobre los MSB, preguntas frecuentes (Frequently Asked Questions, FAQ) sobre los MSB e información/herramientas útiles para los MSB.

La sección de enlaces rápidos proporciona acceso a un documento muy importante e informativo denominado “MSB Examination Manual” (Manual de examen del MSB). Este documento proporciona un resumen de los requisitos de cumplimiento de la Ley de Secreto Bancario/Normas contra el lavado de dinero (BSA/AML) y procedimientos de examen para el sector de los MSB. Contiene una visión general de los requisitos del programa de AML, las expectativas de riesgo de BSA/AML y de control de riesgo, buenas prácticas del sector y procedimientos de examen.

** La FinCEN es propietaria del contenido de este sitio web y lo administra. La información/localidad puede cambiar sin aviso.*

¿Es necesario que me inscriba como Negocio de Servicios Monetarios (siglas en Inglés MSB)?

Si participa en actividades de MSB según se define en la **BSA**, debe trabajar con su representante de MoneyGram para determinar su requisito de inscribirse electrónicamente por Internet como un **MSB** en el **Departamento del Tesoro de los EE. UU.**

Consulte la **Sección 6, Inscripción del MSB***, de esta carpeta de recursos para obtener más ayuda.*

Creación de un programa de cumplimiento contra el lavado de dinero

Las reglamentaciones de la **BSA** y de la **Ley PATRIOTA de los EE. UU.** requieren que todos los **MSB** adopten un ***programa de cumplimiento*** formal y escrito contra el lavado de dinero, razonablemente elaborado para garantizar el mantenimiento de registros y la presentación de informes adecuados de determinadas transacciones y para evitar que su empresa sea utilizada para lavar dinero. Como mínimo, su programa de cumplimiento contra el lavado de dinero debe incluir lo siguiente:

A. La designación de un Oficial de cumplimiento que sea responsable de asegurar que ocurre lo siguiente:

- Se cumplan las políticas y los procedimientos.
- Se actualizan los procedimientos según sea necesario.
- Se proporcionan capacitación y educación.
- Se presentan en forma adecuada los informes.

B. Políticas, procedimientos y controles internos para lo siguiente:

- La verificación de la identidad del cliente.
- El monitoreo de transacciones.
- La presentación de informes.
- La creación y la conservación de registros de todas las transacciones.
- La respuesta a las peticiones de la autoridad policial.

C. Un programa de capacitación de empleados continuo que realice lo siguiente:

- Explique las políticas y los procedimientos.
- Enseñe cómo identificar actividades sospechosas.
- Identifique cómo y dónde se presentan y guardan permanentemente los registros de capacitación.

D. Una revisión independiente del programa contra el lavado de dinero:

- La frecuencia y la extensión de la revisión del programa contra el lavado de dinero deben depender de los riesgos de cumplimiento específicos de su empresa. La “mejor práctica” consiste en realizar una revisión al menos una vez al año. Sin embargo, es posible que se soliciten más revisiones, si corresponde.
- La revisión puede ser realizada por uno de sus empleados, pero **no la puede** realizar el Oficial de cumplimiento, nadie que dependa de él ni un representante de MoneyGram.

***La Sección 2, Programa de cumplimiento**, de este recurso brinda pautas adicionales para establecer el programa de cumplimiento.*

¿Cuáles son los requisitos de verificación del documento de identificación del cliente?

Envíos de dinero

Antes de realizar cualquier envío de dinero que sea por el monto de $900.00 o más, debe confirmar la identidad del cliente. Para ello, **solicite y revise** un documento de identificación con foto, válido, emitido por el gobierno, que contenga el nombre y la dirección de la persona, como una licencia de conducir válida (vigente) u otra credencial de identificación emitida por el gobierno. *Si el cliente **no es** residente de los EE. UU., deberá presentar un pasaporte, una tarjeta de identificación de extranjero u otro documento oficial que refleje su nacionalidad o residencia.*

En todos los casos de RECEPCIÓN de envíos de dinero, *independientemente de la cantidad*, **DEBE CONFIRMAR LA IDENTIDAD DEL CLIENTE.** Se permiten las preguntas de prueba y respuestas aceptables en el caso de *envíos de dinero de* **hasta $899** si el beneficiario no tiene un documento de identificación con foto aceptable. Los detalles de la identificación o la respuesta a la pregunta de prueba **deben registrarse** para las transacciones de **RECEPCIÓN** de dinero.

Requisitos adicionales de identificación del cliente para el envío de dinero

Tanto los agentes que realizan envíos de dinero como los que los reciben deben obtener y **REGISTRAR** información específica de la identificación del cliente para los envíos de dinero, *según* la cantidad de dinero, independientemente del método de pago. El cliente debe estar físicamente presente en su localidad cuando se realiza la transacción, de manera que pueda obtener y verificar la información sobre la identidad del cliente. Utilice la siguiente tabla para determinar qué información debe registrar: *(Consulte la página siguiente para obtener información sobre las transacciones de terceros [en nombre de otra persona]).*

	$0.01 - $899.99	$900.00 - $2,999.99	$3000.00 - $10,000.00*
Nombre	X	X	X
Dirección	X	X	X
Monto de la transacción	X	X	X
Fecha de la Transacción	X	X	X
Documento de identificación con foto válido emitido por el gobierno. *(Consulte la información anterior si no es residente de los EE: UU.)*		X	X
Número de seguro social o número de identificación fiscal. *(Consulte la información anterior si no es residente de los EE. UU.)*			X
Fecha de nacimiento			X
Ocupación específica			X

** **Antes** de completar transacciones únicas o múltiples por un total de **más de $9,100**, **DEBE** ponerse en contacto con Operaciones contra el lavado de dinero de MoneyGram al 1-800-444-3010 (seleccione la opción 7).*

Máximo total de transacciones

La cantidad máxima total permitida **por transacción** de envío es de $10,000. Sin embargo, antes de continuar con cualquier cantidad de $9,100 o más, debe llamar al 1-800-444-3010 y seleccionar la opción 7 para una entrevista con el remitente. Este proceso podría tardar de 30 a 45 minutos.

MoneyGram limita a los clientes a un máximo total de envío de $20,000 por día, sujeto al mismo proceso detallado arriba.

Requisito de conservación de registros de transacción

Debe conservar los documentos físicos de todos los envíos de dinero por $3,000 o una cantidad superior durante cinco (5) años.

Requisitos de identificación del cliente para transacciones con giro postales

Si el mismo cliente compra $3,000 o más en giro postales con efectivo, en el mismo día, **DEBE** obtener y registrar la siguiente información de la transacción del cliente en el diario de giro postales **ANTES** de completar las transacciones:

- Nombre y dirección de la **localidad** en la que se compró el giro postal.
- Nombre y dirección del **cliente** que compró el giro postal.
- Fecha en la que el cliente compró el giro postal.
- Ocupación/empleo del cliente que compró el giro postal.
- Número de seguro social o número de identificación fiscal del cliente que compró el giro postal.

  *Si el cliente **no es** residente de los EE. UU., deberá presentar un pasaporte, una tarjeta de identificación de extranjero u otro documento oficial que refleje su nacionalidad o residencia.*
- Fecha de nacimiento de la persona que compró el giro postal.
- Tipo de documento de identificación con foto válido y emitido por el gobierno *(p. ej., licencia de conducir de TX)* y el número de la identificación.
- *Monto TOTAL de TODOS los giro postales que compró el cliente.*
- Números de serie de **CADA** giro postal.

  (Deben aparecer todos los dígitos. El uso de caracteres como “XXX” para omitir este requisito no está permitido).
- Monto de **CADA** giro postal que se compró.

Una nota acerca de transacciones de terceros (en nombre de otra persona)

Si usted sabe que el cliente envía/recibe dinero o compra un giro postal en nombre de otra persona, debe obtener también la misma información de esa otra persona. Un ejemplo de esto sería un familiar de una persona mayor que realiza una transacción de recepción para esta última (ambas personas DEBEN ESTAR físicamente en su localidad) o el del empleado que realiza la transacción para la empresa en la que trabaja.

¿Cuáles son los requisitos para la presentación electrónica del Informe de Transacciones en Divisas (siglas en Inglés CTR)?

Las transacciones en efectivo superiores a $10,000 realizadas en un mismo día, por cualquier persona, o en nombre de otra persona, **REQUIEREN** la presentación electrónica de un ***CTR*** ante el gobierno federal a través del sistema de presentación electrónica de la FinCEN*. El límite de $10,000 incluye tanto el valor nominal de la transacción como las demás tarifas que paga el cliente.

Las compras en efectivo de giro postales o envíos de dinero múltiples se deben tratar como un total si usted sabe que las transacciones las realiza la misma persona o se realizan en nombre de la misma persona y que suman más de $10,000 en el mismo día hábil.

Requisitos de presentación electrónica del CTR (Título 31 del Código de reglamentaciones federales)

- Debe hacer la presentación electrónica del CTR en los 15 días posteriores a la transacción mediante el sistema de la FinCEN.
- NO envíe el CTR a MoneyGram.
- Debe imprimir y conservar una copia de cada CTR presentado en forma electrónica, o tener acceso a ella, durante al menos cinco (5) años.

* Consulte la Sección 7, Presentación electrónica del CTR, para consultar los procedimientos de presentación electrónica del CTR de la FinCEN.

NOTA: *Los CTR y otros registros e informes son válidos únicamente en función de la información proporcionada por usted. Por lo tanto, es muy importante que en dichos informes se proporcione información precisa y completa. Esa es su responsabilidad. El gobierno y las fuerzas de policía dependen de esta información para luchar contra el lavado de dinero, el fraude y el terrorismo.*

¿Qué es una actividad sospechosa?

Las “actividades sospechosas” pueden variar de transacción en transacción, según las circunstancias que rodeen la transacción o el grupo de transacciones.

Por ejemplo, las transacciones que realiza un cliente pueden ser normales, debido a que usted conoce a ese cliente. Sin embargo, las mismas transacciones realizadas por otro cliente menos frecuente pueden ser sospechosas. Hay muchos factores involucrados en determinar si una transacción es sospechosa, entre los que se incluyen los siguientes:

- Cantidad de la transacción.
- Localidad de la empresa.
- Localidad de la empresa.

Es importante que usted y todos sus empleados lean y conozcan el material de este recurso para que los ayude a detectar actividades sospechosas relacionadas con todas las transacciones de servicios monetarios.

Ejemplos de actividades sospechosas varias:

Ejemplo 1: Un cliente dice que quiere enviar $5,000 y quiere pagar con dinero en efectivo. Cuando le explica al cliente que necesita su información de identificación personal, este le pregunta qué cantidad de dinero puede enviar sin necesidad de mostrar su documento de identificación. Usted debe presentar un SAR de forma electrónica sobre la transacción o el intento de transacción.

Ejemplo 2: Un cliente compra giro postales con dinero en efectivo por una cantidad apenas inferior a $3,000 en el transcurso de varios días. Puede que el cliente esté estructurando sus compras. Debe considerar presentar un SAR electrónicamente.

Ejemplo 3: Usted ve cómo Jim le entrega dinero en efectivo a Bill y Susan fuera de su tienda. Bill y Susan le entregan a usted dinero en efectivo y compran giro postales por un total inferior a $900 cada uno, pero que juntos suman más de $900. Esto parece ser una transacción estructurada y es posible que sea necesario presentar en forma electrónica un SAR y registrar la compra en el diario de giro postales.

Ejemplo 4: Un cliente retira un envío de dinero de su localidad. Después de que se fue, descubre que el mismo cliente también retiró envíos de dinero en otras oficinas de su agencia en el mismo día. Puede que el cliente esté tratando de evitar los requisitos de mantenimiento de registros y presentación de informes. Si sospecha que se produjo una actividad sospechosa o estructurada, debe presentar un SAR en forma electrónica por el total de todas las transacciones. Si el monto total de las divisas pagadas al cliente supera los $10,000 en un día, también debe presentar un CTR.

Ejemplo 5: Un cliente retira un envío de dinero en su localidad, que está ubicada en la frontera de los EE. UU., y lo acompaña otra persona. La otra persona parece decirle al cliente qué hacer. Una vez que se completa la transacción, el cliente le da el dinero a la otra persona. El cliente puede estar pagando para hacer ingresar a un miembro de la familia o a un amigo en forma clandestina por la frontera. Debe presentar un SAR en forma electrónica sobre la transacción o el intento de transacción.

Nota:

Los ejemplos anteriores representan solo algunas de las distintas situaciones posibles o tipos de transacciones que podrían levantar sospechas y no deben considerarse como regla para todos los casos. Puede encontrar ejemplos adicionales en www.fincen.gov. Si tiene inquietudes sobre lo que parece ser una actividad sospechosa, no dude en comunicarse con MoneyGram por teléfono al 1-800-444-3010 y seleccione la opción 7.

¿Cuáles son los requisitos de la presentación electrónica del Informe de Actividad Sospechosa (siglas en Inglés SAR)?

CUALQUIER transacción que parezca sospechosa **REQUIERE** la presentación electrónica de un ***SAR*** ante el gobierno federal a través del sistema de presentación electrónica de la FinCEN*. Estos tipos de transacciones incluyen, a título enunciativo, las siguientes condiciones:

1. Involucran fondos que sospecha que provienen de actividades ilegales o delictivas o cuyo objetivo es ocultar fondos derivados de actividades ilegales o delictivas.
2. Parecen estar estructuradas para evitar requisitos de presentación de informes o mantenimiento de registros.
3. Parecen no tener un fin comercial o legítimo aparente.

Requisitos de presentación electrónica del SAR

- Debe hacer la presentación electrónica del **SAR** en los **30 días** posteriores a la detección de la actividad sospechosa.
- NO envíe el informe a MoneyGram.
- Debe imprimir y conservar una copia de cada **SAR** presentado electrónicamente y toda la documentación de respaldo, o tener acceso a ellos, durante al menos cinco (5) años
- **Nunca le diga a su cliente que presentó electrónicamente un SAR.**

  Nota: Es ilegal decirle al cliente que va a presentar electrónicamente un SAR-MSB. Si MoneyGram cree que alguno de sus clientes está haciendo un uso incorrecto de los giro postales o de los envíos de dinero, es posible que nuestro personal dedicado al cumplimiento se ponga en contacto con usted como parte de una investigación. Tampoco debe contarle al cliente sobre este tipo de averiguación.

**** Consulte la Sección 8, Presentación electrónica del SAR, para ver los procedimientos de presentación electrónica del SAR de la FinCEN.***

NOTA: *Los SAR y otros registros e informes son válidos únicamente en función de la información proporcionada por usted. Por lo tanto, es muy importante que en dichos informes se proporcione información precisa y completa. Esa es su responsabilidad. El gobierno y las fuerzas de policía dependen de esta información para luchar contra el lavado de dinero, el fraude y el terrorismo.*

¿SAR o CTR?

La presentación electrónica de un **SAR** es un requisito distinto de la presentación electrónica de un **CTR**. Aun cuando haya presentado un CTR por una transacción o grupo de transacciones, también debe presentar un SAR en forma electrónica, si considera que la actividad es sospechosa.

¿Qué es la estructuración?

Las personas que se dedican al lavado de dinero conocen los límites que exigen el mantenimiento de registros y la presentación de informes. Por lo tanto, para permanecer en el anonimato y evitar ser detectados por las fuerzas policiales, “estructuran” sus transacciones a fin de no tener que cumplir con los requisitos de mantenimiento de registros y presentación de informes. La estructuración consiste en dividir posibles transacciones de mayor tamaño en varias más pequeñas para evitar los requisitos de mantenimiento de registros o de presentación de informes.

¿Qué debo hacer si sospecho de una estructuración?

Es ilegal que los clientes o usted estructuren las transacciones a fin de evitar los requisitos de mantenimiento de registros o presentación de informes.

Por ejemplo, si un cliente realiza un envío de $1,500 a la mañana y otro de $1,500 a la tarde, puede que esté estructurando sus operaciones a fin de evitar los requisitos de mantenimiento de registros de los $3,000.

Es ilegal que sus clientes o sus empleados ayuden a otra persona a estructurar las transacciones a fin de evitar los requisitos de mantenimiento de registros o presentación de informes. Por ejemplo, no puede decir ni sugerir a los clientes que pueden evitar proporcionar información mediante la realización de transacciones menores. Algunos delincuentes pueden tratar de engañarlos a usted o a sus empleados para que les permitan estructurar una transacción dividiendo la actividad entre varios cómplices o tratando de “estafarlo” con una historia de infortunio. Debe estar atento ante cualquier sospecha de estructuración para evitar que se concrete.

¿Se consideran estructuración todas las transacciones múltiples?

No.

Por ejemplo, un cliente realiza dos envíos de dinero a diferentes beneficiarios, uno por $2,000 y otro por $1,500. Cada envío es inferior a $3,000, pero el total de la transacción supera los $3,000. Usted se entera de que el cliente envía dinero a sus hijos que asisten a distintas escuelas.

Este también es un ejemplo de la documentación de revisión de la transacción que debe hacer y conservar como parte de su programa de **MONITOREO.**

Política de datos

Como agente, debe proteger toda información personal que no sea pública. Solo puede recopilar y solicitar la información de identificación personal que sea necesaria para completar la transacción.

De acuerdo con la *Norma de salvaguarda de la Ley Gramm–Leach–Bliley de la Comisión federal de comercio*, usted debe salvaguardar de manera adecuada la información personal no pública. Esto incluye implementar políticas escritas con respecto a la recopilación y a la divulgación de información del cliente considerada “información personal no pública” y designar un empleado o más para que coordinen el programa de seguridad de la información. Consulte el **sitio web de la FTC** para obtener ayuda adicional a fin de crear el programa de seguridad de la información, www.business.ftc.gov/privacy-and-security.

Otros consejos incluyen, de forma no taxativa, los siguientes:

- Evitar hacer referencia a los datos de identificación en voz alta, como direcciones, números de teléfono, números de seguro social, etc., cuando otras personas puedan escuchar lo que dice.
- Nunca muestre la pantalla del monitor del sistema de MoneyGram a ningún cliente.
- Cualquier nota, formulario, diario u otro documento que contenga información personal no pública del cliente debe destruirse antes de proceder a deshacerse del documento.

Conservación de registros

Todo el material de mantenimiento de registros y de presentación de informes requerido por la Ley de Secreto Bancario (Bank Secrecy Act, BSA) y las reglamentaciones específicas del estado se mantendrán durante al menos cinco (5) años y se pondrán a disposición inmediata del Departamento del Tesoro de los EE. UU. y/o los representantes de otros funcionarios de gobierno ante solicitud legítima.

La ley exige que conserve los recibos de todas las transacciones de $3,000 o más durante al menos cinco (5) años.

Privacidad del cliente
De acuerdo con la Ley de Privacidad, debe proteger la información personal y privada de los clientes. Todos los documentos que contengan información personal y privada de los clientes deberán almacenarse en un lugar seguro. Si desea descartar legalmente cualquier documento relacionado con el MSB o MoneyGram, debe destruirlo por completo antes de desecharlo.

Uso personal de los servicios

Como agente de MoneyGram, no debe iniciar, procesar ni completar ningún servicio monetario personal de MoneyGram en su nombre ni en nombre de sus familiares directos.