POLÍTICA CONTRA EL LAVADO DE DINERO ("AML"), FINANCIACIÓN ANTITERRORISTA ("CTF") Y DELITOS FINANCIEROS

1. POLÍTICA

1.1 Crixto Limited (la "Compañía") está expuesta al riesgo de que delincuentes busquen utilizar las actividades comerciales de la Compañía para el lavado de dinero y cometer otros delitos financieros. La Compañía y todos sus empleados están sujetos a las leyes contra el blanqueo de dinero y la financiación del terrorismo, en particular la Ley de Procedimientos contra el Delito de 2002 ("POCA 2002") y la Ley de Terrorismo de 2000 ("TA 2000").

2. CUMPLIMIENTO

2.1 Se espera que todos los empleados de la Compañía se familiarizen con esta política y la cumplan.

2.2 El cumplimiento estricto de las disposiciones de esta política y otras normas sobre la lucha contra el blanqueo de dinero y la financiación antiterrorista son una condición de empleo por parte de la Compañía. Cualquier incumplimiento de esta política y tales reglas puede dar lugar a que se adopten procedimientos disciplinarios contra cualquier director o empleado pertinente, además puede exponer al individuo en cuestión al riesgo de ser procesado penalmente. En particular, es probable que el hecho de no informar sobre el conocimientos o sospechas de blanqueo de dinero al Oficial de Cumplimiento ("CO") sea probablemente un delito penal, y que se considere una falta grave que puede dar lugar a un despido inmediato sin pago. La junta directiva, con la asistencia del CO, es responsable de iniciar y supervisar la investigación de todos los informes de incumplimientos de esta política y otras normas y de garantizar que se tomen las medidas disciplinarias apropiadas cuando sea necesario.

3. ¿QUÉ ES EL LAVADO DE DINERO?

3.1 El Grupo de Acción Financiera ("FATF", por sus siglas en inglés) – un organismo intergubernamental de el cual el Reino Unido es miembro, y que trabaja para combatir el lavado de dinero y la financiación del terrorismo – define el lavado de dinero de la siguiente manera:

3.2 "El objetivo de un gran número de actos delictivos es generar un beneficio para el individuo o grupo que lleva a cabo el acto. El lavado de dinero es el procesamiento de estos ingresos criminales para ocultar su origen ilegal. Este proceso es de vital importancia, ya que permite al criminal disfrutar de estos beneficios sin poner en peligro su fuente..."

3.3 "Cuando una actividad delictiva genera beneficios sustanciales, el individuo o grupo involucrado debe encontrar una manera de controlar los fondos sin llamar la atención sobre la actividad subyacente o las personas involucradas. Los delincuentes hacen esto disfrazando las fuentes, cambiando la forma o moviendo los fondos a un lugar donde es menos probable que atraigan la atención. ″

3.4 Por lo general, el lavado de dinero se produce en varias etapas.

3.4.1 En primer lugar, en la etapa inicial -o colocación-, el blanqueador introduce sus ganancias ilegales en el sistema financiero. Esto podría hacerse dividiendo grandes cantidades de efectivo en sumas más pequeñas menos visibles que luego se depositan directamente en una cuenta bancaria, o comprando una serie de instrumentos monetarios (cheques, giros postales, etc.) que luego se recogen y depositan en cuentas en otro lugar.

3.4.2 En segundo lugar, después de que los fondos han entrado en el sistema financiero, se lleva a cabo una fase de capas. En esta fase, el blanqueador participa en una serie de

conversiones o movimientos de los fondos para distanciarlos de su fuente. Los fondos podrían canalizarse a través de la compra y venta de instrumentos de inversión, o el blanqueador podría simplemente transferir los fondos a través de una serie de cuentas en varios bancos de todo el mundo. Este uso de cuentas ampliamente dispersas para el lavado es especialmente frecuente en aquellas jurisdicciones que no cooperan en investigaciones contra el lavado de dinero. En algunos casos, el blanqueador podría disfrazar las transferencias como pagos por bienes o servicios, dándoles así una apariencia legítima.

3.4.3 En tercer lugar, después de haber procesado con éxito los beneficios delictivos a través de las dos primeras fases, el blanqueador los traslada a la tercera etapa, la integración, en la que los fondos vuelven a entrar en la economía legítima. El blanqueador podría optar por invertir los fondos en bienes raíces, activos de lujo o empresas.

3.5 La Compañía, a través de su aceptación de criptomonedas a cambio de saldos almacenados electrónicamente de moneda fiduciaria que se pueden utilizar para la compra de bienes y servicios, está particularmente expuesta a la segunda y tercera etapa del lavado de dinero.

4. EVALUACIÓN DE RIESGOS

4.1 De acuerdo con la orientación de la industria, la Compañía entiende que sus medidas contra el blanqueo de dinero y los delitos financieros deben ser proporcionales al nivel de riesgo, y diseñadas para mitigar y gestionar los riesgos específicos inherentes tanto a su negocio como a los transacciones en las que está involucrada. A tal efecto, la Compañía ha llevado a cabo una evaluación de riesgos de AML y CTF para identificar riesgos para sus negocios, y actividades comerciales particulares que tienen mayores riesgos.

4.2 Esta evaluación se lleva a cabo de forma continua y se actualiza según corresponda en función de los cambios en el negocio y sus operaciones. Un resumen de las evaluaciones de riesgos actuales es el siguiente:

Evaluación global del riesgo

4.3 Teniendo en cuenta la orientación del FATF y otra información disponible, la Compañía evalúa el riesgo de que su negocio de intercambio de criptodivisas y transferencia de valor esté sujeto al lavado de dinero o financiamiento del terrorismo como moderado. Los productos que ofrece la Compañía son, por su naturaleza, potencialmente atractivos para los blanqueadores de dinero (ver más abajo), aunque en el extremo inferior del espectro de riesgo relevante para esta industria.

4.4 Las actividades de la Compañía que están expuestas al mayor riesgo de delitos financieros son la actividad principal del negocio y se llevan a cabo de forma rutinaria y de gran volumen. Si bien la Compañía no recibe dinero en efectivo de los clientes, sí recibe activos que pueden haber sido comprados utilizando propiedades criminales, luego convierte dichos activos en valor monetario que se puede intercambiar por bienes y servicios. En estas circunstancias, el riesgo de AML para la Compañía asociado con estas actividades es materialmente el mismo que el riesgo de AML asociado con la recepción de efectivo directamente de los clientes y la transferencia de ese efectivo a terceros. El grado relativo de anonimato involucrado en los criptoactivos, así como el hecho de que los criptoactivos no están vinculados a jurisdicciones específicas y los canales de distribución utilizados aumenta los factores de riesgo para la Compañía.

Factores de riesgo del cliente

4.5 Los clientes de los servicios de la Compañía están principalmente restringidos, en práctica, a los individuos, pero hay ciertos clientes corporativos. Los clientes pueden estar potencialmente

basados en cualquier ubicación y no están restringidos en su clasificación regulatoria (es decir, la Compañía podría tratar con los consumidores minoristas que llevan a cabo intercambios únicos, así como usuarios de criptoactivos profesionales que llevan a cabo intercambios regulares). Como los criptoactivos no son un activo de inversión común, y tratar de convertirlos moneda fiduciaria no es un servicio típico, es poco probable que los clientes de la Compañía puedan ser vistos como tener un perfil de riesgo equivalente a otros usuarios de dinero electrónico y remesas de dinero

4.6 Como se identifica en la Evaluación de Riesgos AML de la Compañía, existe potencialmente un riesgo de que las entidades de la Compañía entren en contacto con "personas políticamente expuestas" (como se define en el Reglamento de Blanqueo de Capitales, Financiamiento del Terrorismo y Transferencia de Fondos (Información sobre el Pagador) 2017("MLRs 2017")) durante el curso de su negocio, aunque esto es relativamente bajo.

4.7 Otro riesgo potencial es que la Compañía no tenga relaciones continuas con los clientes, con algunos clientes potencialmente participando en transacciones únicas con la Compañía. Por lo tanto, esto limita la oportunidad de la Compañía de recolectar una gama de datos sobre el cliente y sus transacciones para ayudar a identificar tendencias sospechosas. Esto se ve algo mitigado por el hecho de que los intercambios estarán directamente relacionados con el poder adquisitivo como comerciantes específicos, dando así una imagen clara de a quién se transferirá el valor de los criptoactivos en última instancia, aunque no mitiga completamente el riesgo.

Países y factores de riesgo geográficos

4.8 Las actividades de la Compañía podrían tener vínculos con jurisdicciones de alto riesgo. La propia Compañía lleva a cabo sus actividades en el Reino Unido, aunque los clientes y los activos transferidos pueden proceder de jurisdicciones fuera del Reino Unido y del EEE. Por lo tanto, la Compañía está directamente expuesta a jurisdicciones extranjeras (incluyendo miembros que no son miembros del FATF).

4.9 La Compañía ha tomado medidas para evitar que sus servicios sean accedidos por personas ubicadas en países de la lista de "terceros países de alto riesgo" identificada por la Comisión Europea.

Factores de riesgo de productos, servicios, transacciones y canales de entrega

4.10 Los servicios que ofrece la Compañía son, por su naturaleza, potencialmente atractivos para los blanqueadores de dinero como medio de colocar, estratificar o integrar fondos lavados en el Reino Unido. Los servicios ofrecidos por la Compañía permiten a los clientes encubrir activos que potencialmente han sido adquiridos ilegalmente o mediante el uso de ganancias criminales en lo que es equivalente a la moneda fiduciaria, y luego utilizarlos para comprar activos y/o servicios, agregando así otra capa de transacciones. También permite que el valor inherente a los criptoactivos se transfiera a un tercero bajo el pretexto de una transacción comercial legítima. Este factor se complementa con el hecho de que los criptoactivos, por su naturaleza, tienen datos muy limitados disponibles con respecto a su origen específico y las partes involucradas en su generación. Por lo tanto, esto limita sustancialmente la capacidad de la Compañía para rastrear la fuente de los activos y obtener evidencia de sus orígenes legítimos.

4.11 Además, como este negocio opera únicamente en línea, por lo tanto, no hay interacción cara a cara con los clientes. Esto aumenta la dificultad para verificar la identidad de los clientes y el riesgo de suplantación/fraude.

4.12 Dicho esto, como las transacciones finales deben estar conectadas a comerciantes previamente aprobados, por lo tanto, hay limitaciones sustantivas sobre dónde se puede transferir el valor

inherente a los activos criptográficos. Esto reduce la probabilidad de que la Compañía sea utilizada para facilitar delitos financieros en cierta medida, aunque no completamente dado que la Compañía todavía podría ser utilizado para la integración / extracción de propósitos de valor.

4.13 En conjunto, estos factores sugieren que el riesgo de que el negocio de la Compañía se utilice específicamente para fines de lavado de dinero o financiación del terrorismo es moderado.

5. TRANSACCIONES CON ENLACES A "TERCEROS PAÍSES DE ALTO RIESGO"

5.1 La política de la Compañía es no celebrar ninguna transacción o acuerdo que tengan algún enlace a determinados países que la Comisión Europea identifica como "terceros países de alto riesgo", sin el permiso previo por escrito del CO para gestionar su riesgo de delito financiero. La lista actual de países de alto riesgo es: Afganistán, Bosnia y Herzegovina, Guyana, Irak, RDP Lao, Siria, Uganda, Vanuatu, Yemen, Etiopía, Sri Lanka, Trinidad y Tobago, Túnez, Pakistán, Irán y Corea del Norte. Una versión consolidada de la lista de terceros países de alto riesgo está disponible en el sitio web de la Comisión Europea aquí. Las transacciones/acuerdos con vínculos con esos países (por ejemplo, porque un posible inversor es residente de uno de ellos o está establecido en uno de ellos) deben considerarse como un alto riesgo de blanqueo de dinero y financiación del terrorismo.

6. EL OFICIAL DE CUMPLIMIENTO ("CO")

6.1 Bajo POCA 2002, la Compañía está obligada a tener un "oficial nominado" para recibir informes de conocimientoy/o sospecha de lavado de dinero. La Compañía se refiere a la persona que realiza este papel como el CO. Esa persona recibirá informes de presunto lavado de dinero de los empleados de la Compañía.

6.2 El CO también proporcionará asesoramiento sobre asuntos relacionados con la lucha contra el lavado de dinero y financiación del terrorismo a los empleados de la Compañía, y debe ser el primer punto de contacto para los empleados de la Compañía que tengan preocupaciones sobre cualquiera de estos asuntos, o que necesiten hacer un informe de lavado de dinero, incluso si no trabajan dentro de las partes reguladas del negocio de la Compañía.

7. COMPRENDER LOS PRINCIPALES DELITOS DE BLANQUEO DE DINERO DEL REINO UNIDO

¿Qué es "propiedad criminal"?

7.1 En el Reino Unido, las principales infracciones del blanqueo de dinero están contenidas en POCA 2002. Se aplican a la Compañía y a todos los empleados de la Compañía (no solo a los Empleados del Sector Regulado). Dependen del concepto clave de "propiedad criminal". Esto se define muy ampliamente.

7.2 "Propiedad criminal" es cualquier beneficio (monetario o de otro tipo) obtenido de una "conducta criminal", o cualquier propiedad que represente la misma (en su totalidad o en parte, y ya sea directa o indirectamente), siempre que el presunto delincuente conozca o sospeche que la propiedad es o representa tal beneficio.

7.3 "Conducta criminal" es una conducta que:

7.3.1 constituye un delito en el Reino Unido (por ejemplo, fraude, soborno o robo); O

7.3.2 constituiría un delito en el Reino Unido si ocurriera allí.

7.4 No importa:

7.4.1 quien llevó a cabo la conducta delictiva; o

7.4.2 quienes se benefició de ella; o

7.4.3 cuando ocurrió.

7.5 En el contexto del negocio de la Compañía, a modo de ejemplo:

7.5.1 Las inversiones adquiridas por una persona que pagó a la Compañía utilizando ingresos provenientes de un fraude en el Reino Unido podrían constituir "propiedad criminal";

7.5.2 Del mismo modo, acciones por las que un inversor ha pagado en parte de una fuente legítima, y en parte utilizando propiedad criminal producto de un fraude en el Reino Unido, también podrían constituir "propiedad criminal"; Y

7.5.3 La Compañía que procesa una compra o venta de acciones podría incurrir en una transferencia de "propiedad criminal" a la Compañía (la propiedad en sí, o el producto de la venta).

Conducta criminal que tuvo lugar en el extranjero

7.6 Los empleados de la empresa no deben asumir que la conducta en el extranjero no puede dar lugar a "propiedad criminal" en el Reino Unido, o un delito de lavado de dinero en el Reino Unido. Este no es el caso. Sujeto a ciertas excepciones limitadas, el manejo de los ingresos de un delito cometido en el extranjero puede constituir lavado de dinero en el Reino Unido.

Los delitos sustantivos de blanqueo de dinero en LA POCA de 2002

7.7 Los principales delitos de blanqueo de capitales en POCA 2002 son muy amplios y, en la práctica, abarcan la mayoría de las actividades relacionadas con la "propiedad criminal". Los delitos son:

7.7.1 s327 POCA 2002: Se comete un delito si una persona oculta, disfraza, convierte, transfiere o retira bienes criminales de Inglaterra y Gales.

7.7.2 s328 POCA 2002: Un delito se comete cuando una persona entra o se involucra en un acuerdo teniendo el conocimiento o sospecha de que este facilitará a otra persona para adquirir, retener, utilizar o controlar propiedad criminal.

7.7.3 s329 POCA 2002: Se comete un delito cuando una persona adquiere, utiliza o tiene posesión de propiedad criminal.

7.8 En el contexto del negocio de la Compañía, a modo de ejemplo, una transacción en la que un cliente está vendiendo criptoactivos cuando se sabe o se sospecha que el cliente ha utilizado "propiedad criminal" para pagar por esos criptoactivos podría implicar potencialmente la comisión de todos los delitos anteriores:

7.8.1 el delito s327 podría ser cometido por el inversionista – ya que "propiedad criminal" sería transferida de una forma a otra cuando los criptoactivos se venden a cambio del saldo de la moneda fiduciaria;

7.8.2 el delito s328 podría ser cometido por la Compañía a través del procesamiento de la transacción – el proceso de la generación del saldo en moneda fiduciaria probablemente se consideraría como un "acuerdo" que facilitó la retención o el uso de la propiedad criminal por parte del cliente;

7.8.3 el delito s329 podría ser cometido potencialmente por la Compañía que recibe los criptoactivos y por lo tanto adquirido, utilizó o poseyó 'propiedad criminal'.

Sanciones

7.9 Los delitos de blanqueo de dinero en POCA 2002 son muy graves y pueden ser enjuiciados ante un tribunal penal. La pena máxima para la **comisión de cualquiera de ellos es de 14 años de prisión, una multa ilimitada, o ambos.**

Evitar la comisión de los delitos

7.10 La forma principal de evitar que el negocio de la Compañía se utilice para el lavado de dinero (y por lo tanto para evitar que un empleado de la Compañía cometa un delito) es:

7.10.1 llevar a cabo una "Diligencia Debida del Cliente" ("CDD", por sus siglas en ingles) por cada cliente y de acuerdo con su nivel el riesgo, de modo que los intentos reales o sospechosos de utilizar los servicios de la Compañía para delitos financieros puedan ser identificados inmediatamente;

7.10.2 realizar un monitoreo continuo de transacciones para identificar cuando una transacción es sospechosa a la luz de los datos que la Compañía tiene y, por lo tanto, puede requerir que se realice una CDD adicional del cliente;

7.10.3 que los empleados hagan un informe al CO lo antes posible, de la manera explicada más adelante en esta política; y

7.10.4 cuando haya conocimiento o sospecha de delito financiero, que la transacciones que superen el nivel de riesgo aceptado por la Compañía sean rechazada.

7.11 El CO está sujeto a un estatuto legal específico que establece que cuando:

7.11.1 sabe o sospecha que alguien está involucrado en el lavado de dinero;

7.11.2 la información u otro asunto en el que se base su conocimiento o sospecha se obtuvo como consecuencia de una divulgación, hecha por un empleado, de conocimiento/sospecha de blanqueo de dinero; y

7.11.3 conoce o puede identificar (a partir de la información que tiene) a la persona que realiza el lavado de dinero o el paradero de los bienes lavados como consecuencia de la divulgación; o

7.11.4 tiene información que cree, o es razonable esperar que crea, ayudará a identificar a la persona que hace el lavado de dinero o el paradero de la propiedad lavada

entonces deben hacer una divulgación a la ANC sobre el asunto.

7.12 **No hacerlo es una infracción grave por derecho propio del CO. La pena máxima para la comisión de la misma es de 5 años de prisión, una multa ilimitada, o ambos. La Compañía espera que todos los empleados ayuden al CO en el cumplimiento de sus deberes con respecto a la prevención del riesgo de que la Compañía sea utilizada para los fines de delito financiero.**

8. FINANCIACIÓN DEL TERRORISMO

8.1 La Evaluación de Riesgos de la Compañía evalúa su exposición a la financiación del terrorismo como moderada. Los empleados de la empresa deben tener en cuenta los siguientes puntos clave:

8.1.1 la parte 3 de la TA 2000 contiene una serie de delitos que hacen ilegal financiar el terrorismo y utilizar o poseer "propiedad terrorista". Además de los delitos de blanqueo de dinero expuestos anteriormente;

8.1.2 "propiedad terrorista" se define ampliamente para incluir: (a) dinero u otros bienes que puedan utilizarse con fines de terrorismo; (b) los ingresos de la comisión de actos de terrorismo y (c) los ingresos de los actos realizados con fines de terrorismo. Podría incluir potencialmente la propiedad de la Compañía;

8.1.3 la parte 3 de la TA 2000 requiere que los empleados de la Compañía y la Compañía denuncien sospechas de actividades terroristas o tratos en "propiedad terrorista";

si algún empleado de la Compañía tiene alguna sospecha de que las actividades de la Compañía pudieran de alguna manera estar vinculadas al terrorismo o a la financiación del terrorismo, eso es una cuestión de máxima seriedad. El interesado debe dirigirse inmediatamente al CO para informar del asunto y solicitar más asesoramiento. El CO puede buscar asesoramiento legal específico según sea necesario.

9. DELITOS FINANCIEROS

9.1 La Compañía tiene ciertas obligaciones con sus clientes, y bajo la ley del Reino Unido, para evitar que sus servicios se utilicen para fines de una gama más amplia de delitos financieros que el simple lavado de dinero – por ejemplo, la Compañía no debe permitir que sus servicios se utilicen para cometer fraude a terceros.

9.2 Cuando la Compañía y sus servicios se utilizan como cómplice de un delito financiero, además de que la Compañía potencialmente incumple sus obligaciones con sus clientes y bajo la ley del Reino Unido, los ingresos provenientes de estos delitos financieros más amplios muy probablemente estén catalogados como 'propiedad criminal' para los efectos del régimen de blanqueo de dinero.

9.3 Dado que la Compañía participa en los arreglos relacionados con la realización de transacciones con los comerciantes, existe el riesgo de que los comerciantes que en última instancia reciben los fondos puedan tergiversar su identidad, actividades y/o posición financiera, y/o puedan apropiarse indebidamente de los fondos que reciben. La Compañía tiene la obligación de mitigar este riesgo tanto como sea posible.

9.4 En consecuencia, la Compañía ha incorporado elementos a sus procedimientos que le permitirán considerar el riesgo de que pueda ser utilizado con fines fraudulentos por un comerciante, y evaluará la validez de las solicitudes para unirse a los servicios de la Compañía de una manera similar a el CDD llevado a cabo en clientes que buscan intercambiar criptoactivos.

10. REQUISITOS DE AML DE TODOS LOS EMPLEADOS DE LA EMPRESA

Actividades diarias

10.1 Los empleados de la empresa no deben, sin el consentimiento del CO (o una autoridad como la Agencia Nacional del Delito ("NCA"), según corresponda):

10.1.1 ponera a sí mismo, o a la Compañía, en riesgo de cometer uno de los delitos de blanqueo de dinero expuestos anteriormente;

10.1.2 manejar o tratar con cualquier propiedad que sea "propiedad criminal", incluyendo:

(a) aceptar o procesar bienes sospechosos de ser "propiedad criminal";

(b) aceptar la celebración de transacciones u otros acuerdos que se sabe o se sospecha que implican "propiedad criminal";

10.1.3 tratar de manejar "propiedad criminal";

10.1.4 acordar con cualquier persona para manejar "propiedad criminal";

10.1.5 alentar o ayudar a otra persona a manejar "propiedad criminal";

10.1.6 revelar a cualquier otra persona el hecho de que se han informado al CO sobre un posible problema relacionado al lavado de dinero;

10.1.7 revelar a cualquier otra persona el hecho de que se haya hecho un Informe de Actividad Sospechosa ("SAR") al CO o a las autoridades;

10.1.8 revelar a cualquier otra persona el hecho de que se está contemplando o llevando a cabo una investigación de lavado de dinero;

10.1.9 hacer cualquier divulgación que pueda perjudicar una investigación de lavado de dinero; o

10.1.10 falsificar, ocultar, destruir o de alguna otra manera disponer (o causar la falsificación, ocultación, destrucción o eliminación de) documentos que puedan ser relevantes para una investigación de lavado de dinero.

10.2 Hacer cualquiera de lo anterior podría constituir un delito penal por parte del empleado de la Compañía y potencialmente por parte de la Compañía.

10.3 Cualquier empleado de la Compañía que conozca o sospeche que cualquier persona (en cualquier capacidad: un inversionista individual, un empleado de un inversionista corporativo, una parte que busca inversión) está o puede estar involucrado en el uso del negocio de la Compañía para el lavado de dinero debe:

10.3.1 ponerse en contacto con el CO inmediatamente para solicitar asesoramiento y, de ser apropiado, reportar el problema. No debe demorarse, ya que esto puede hacer imposible que el individuo en cuestión, y la Compañía, obtengan una defensa ante un delito de blanqueo de dinero;

10.3.2 mantener un buen registro de la información que ha causado que se preocupen, por ejemplo, cualquier nota hecha durante una reunión o llamada con un abogado o agente cuando se discuta información relevante;

10.3.3 obedecer cualquier instrucción dada por el CO con respecto al asunto, incluyendo cualquier instrucción de no proceder con la actividad o transacción pertinente que pueda implicar el lavado de dinero hasta que las autoridades hayan otorgado el consentimiento.

Procedimientos para hacer frente a las sospechas de blanqueo de dinero

10.4 De vez en cuando:

10.4.1 las empresas de servicios profesionales que asesoran a la Compañía (como abogados o agentes) pueden plantear posibles problemas de lavado de dinero con la Compañía en un contexto transaccional; y/o

10.4.2 un empleado de la Compañía puede, a través del curso de ayudar con una transacción, desarrollar su propio conocimiento o una sospecha de lavado de dinero.

10.5 En tales circunstancias:

10.5.1 los requisitos generales para la gestión de riesgos de AML establecidos en esta política siguen aplicándose, en particular los empleados de la Compañía en cuestión deben ponerse en contacto con el CO inmediatamente para hacer un informe y no deben revelar

a otros (incluidas otras partes de la transacción) el hecho de que se haya presentado un informe a menos que el CO lo autorice;

10.5.2 puede ser necesario que el CO obtenga el consentimiento de las autoridades para que la transacción se realice, sin informar a ninguna otra parte de la transacción (ni permitir que otros lo hagan). Los empleados de la empresa deben obedecer las instrucciones del CO en ese sentido;

10.5.3 si la Compañía ha instruido a asesores profesionales (por ejemplo, cualquier abogado o agente), es probable que esos asesores tengan sus propias obligaciones de hacer informes a las autoridades. Las preocupaciones de los asesores pueden o no ser reveladas a la Compañía. Los empleados de la empresa deben, en el momento en que hagan su propio informe, estar listos para dar los detalles del CO de dichas empresas o individuos que estén asesorando a la Compañía. En algunos casos, un informe conjunto de la Compañía y sus asesores puede ser aconsejable o apropiado. Sin embargo, la comunicación sobre posibles problemas de lavado de dinero con cualquier persona fuera de la Compañía está restringida por la ley y debe ser en la práctica dirigida por el CO o hecha sólo con el consentimiento del CO.

11. OBLIGACIONES DE CDD DEL CLIENTE EN LA COMPAÑÍA

11.1 Con el fin de gestionar su riesgo de delito financiero, la Compañía aplica medidas de CDD al cliente cuando:

11.1.1 establece una relación comercial con un "cliente" (por ejemplo, cuando acepta una solicitud para abrir una cuenta para el intercambio de criptoactivos para un cliente individual/corporativo);

11.1.2 sospecha de blanqueo de dinero, financiación del terrorismo o comportamiento fraudulento, por ejemplo, cuando una transacción es inusualmente grande y/o existe un patrón inusual de transacciones; o

11.1.3 duda de la veracidad o adecuación de los documentos o informaciones previamente obtenidas de sus clientes con el fin de identificarlos.

11.2 Un "cliente" de la Compañía en estas circunstancias significa una persona con la que la Compañía tiene una relación profesional o comercial. En la práctica, es probable que los "clientes" de la Compañía sean (i) individuos o empresas que deseen intercambiar criptoactivos con la Compañía por un saldo en moneda fiduciaria; y (ii) comerciantes dispuestos a aceptar los saldos de divisas fiduciarias como medio de pago.

11.3 En estas circunstancias, la Compañía debe:

11.3.1 identificar al cliente;

11.3.2 "verificar" la identidad del cliente (en el sentido de utilizar documentos obtenidos de una fuente fiable independiente de la persona cuya identidad se está verificando, como el registro público de empresas que se mantiene en la Companies House); y

11.3.3 evaluar y, en su caso, obtener información sobre el propósito y la naturaleza prevista de la relación comercial o transacción ocasional (normalmente, por qué el cliente desea abrir una cuenta, qué se espera que haga la Compañía a ese respecto y con qué frecuencia).

11.4 Cuando el cliente es una empresa, la Compañía está obligada a:

11.4.1 obtener su nombre y su número de empresa u otro número de registro; y

11.4.2 la dirección de su oficina y (si es diferente) el lugar principal de su negocio.

11.5 A menos que el cliente aparezca en un mercado regulado, la Compañía también está obligada a:

11.5.1 tomar medidas razonables para determinar y verificar la ley a la que está sujeta la empresa, y su constitución;

11.5.2 los nombres completos de su junta directiva y de la persona con mayor responsabilidad sobre sus operaciones;

11.5.3 cuando sea propiedad beneficiosa de otra persona, identificar al propietario beneficiario y tomar medidas razonables para verificar su identidad de tal manera que la Compañía esté satisfecha de que sabe quién es el propietario beneficiario;

11.5.4 cuando el propietario beneficiario sea una empresa (como suele ser el caso), tomar medidas razonables para entender su estructura de propiedad y control; y

11.5.5 mantener registros escritos de las acciones tomadas para identificar al propietario beneficiario.

11.6 Esta información puede estar disponible públicamente en Company House, o a través de procedimientos normales de CDD.

11.7 La Compañía tendrá que obtener documentación en línea con sus procedimientos CDD, antes de permitir que un cliente utilice sus servicios, o permitir que un comerciante realice transacciones facilitadas por sus servicios. En cualquier caso que se considere que presenta un mayor riesgo de blanqueo de dinero, una CDD más detallada (‘mejorada’) sobre el "cliente" puede que sea requerida. La Compañía debe consultar al CO (y tal vez desee tomar asesoramiento legal separado) en cualquier caso que parezca ser de mayor riesgo.

11.8 Además de lo anterior:

11.8.1 Como se identifica en la Evaluación de Riesgos de AML de la Compañía, diferentes clientes/comerciantes pueden implicar diferentes niveles de riesgo de lavado de dinero dependiendo, en particular, del criptoactivo en cuestión, los países/geografías involucrados y las diversas estructuras corporativas de las partes involucradas. Si bien la Compañía utiliza procedimientos estandarizados para llevar a cabo CDD, la Compañía reconoce que no existe un enfoque "único para todos" para el CDD, y por lo tanto puede alterar el nivel de CDD realizado en un cliente y /o cómo se lleva a cabo este CDD, dependiendo de las circunstancias específicas de la situación.

11.8.2 Cuando información adversa salga a la luz durante el proceso de CDD que no pueda ser abordada satisfactoriamente, la Compañía no procederá a permitir que la entidad relevante tenga acceso a sus servicios. Las sospechas derivadas de la información descubierta durante la CDD deben notificarse al CO como se ha establecido anteriormente;

11.8.3 en todos los casos, independientemente de cualquier otra CDD que se esté haciendo, la Compañía obtendrá un informe (que incluye chequeos sobre personas políticamente expuestas ("PEP") y controles de detección de sanciones) a clientes potenciales en una etapa temprana, para identificar si algún PEP está involucrado y confirmar que no estaría tratando con un individuo o entidad sujeto a sanciones del Reino Unido, la UE, los Estados Unidos o las Naciones Unidas. La Compañía rechazará automáticamente cualquier aplicación en la que el cliente (o un propietario beneficioso del cliente) sea un

PEP. Además, por lo general, tratar con el tema de una sanción financiera o ayudar a una persona a eludir una sanción financiera implicará la comisión de un delito en el Reino Unido. Como resultado, si el informe identifica una posible coincidencia de sanciones, debe ser revisado y aprobado por el CO antes de que se pueda conceder el acceso;

11.8.4 algunos tipos de información adversa detallada en el informe pueden abordarse satisfactoriamente haciendo más consultas al cliente como parte del proceso de CDD. Por ejemplo, la Compañía puede ser capaz de abordar sus preocupaciones confirmando la fuente de riqueza del cliente y que se utilizará una fuente legítima de fondos durante el uso de los servicios de la Compañía;

11.8.5 una revisión de la lista de PEP se llevará a cabo trimestralmente para evaluar si algún cliente actual se ha convertido en un PEP desde que se aprobó por primera vez; y

11.8.6 si surgen sospechas o preocupaciones después de que se haya concedido el acceso, la Compañía puede, no obstante, estar bajo obligaciones de presentación de informes y solicitará asesoramiento legal según corresponda. Si, tras la finalización de un intercambio a través de los servicios de la Compañía, se genera una alerta con información adversa relacionada con una de las partes de la transacción, esta alerta debe ser llevada al CO sin demora. Además, si un empleado de la Compañía tiene conocimiento de cobertura mediática adversa u otra información sobre un cliente y/o una transacción que sugiera que puede haber un problema de lavado de dinero, esto también debe informarse al CO.

12. TIEMPO DE CDD DEL CLIENTE

12.1 La Compañía normalmente debe llevar a cabo la debida diligencia cuando establece la relación comercial con el "cliente". Sin embargo, también debe aplicar medidas de CDD del cliente en otros momentos apropiados, adoptando un enfoque basado en el riesgo, en particular cuando parece que la identidad o propiedad del cliente ha cambiado, la relación no se está utilizando como se pretendía, o pareciera haber algún riesgo de lavado de dinero.

12.2 Cuando la Compañía no pueda aplicar medidas de CDD con el cliente, deberá:

12.2.1 no establecer una relación comercial con el cliente (si corresponde);

12.2.2 no aceptar criptoactivos del cliente;

12.2.3 debe poner fin a cualquier relación comercial existente (si corresponde);

12.2.4 revisar cualquier transacción histórica para determinar si estas presentaban un riesgo de participación en delitos financieros; Y

12.2.5 debe considerar si es necesario presentar un informe al CO.

13. SEGUIMIENTO CONTINUO DE LA RELACIÓN COMERCIAL

13.1 La Compañía lleva a cabo un monitoreo continuo de las relaciones comerciales para asegurar que se utilizan según lo previsto originalmente y de manera consistente con el conocimiento de la Compañía sobre el cliente y el propósito para el cual la relación iba a ser utilizada.

13.2 En el curso normal del negocio, la Compañía debe ser capaz de cumplir con su obligación de llevar a cabo un monitoreo continuo a través de una variedad de tareas relacionadas con el cumplimiento, incluyendo la recolección de datos, filtrado, mantenimiento de registros, gestión de investigaciones e informes.

13.3 Las funcionalidades del sistema incluyen:

13.3.1 Chequeos diarios de los clientes sobre su presencia en las reconocidas"listas negras"(por ejemplo, OFAC),

13.3.2 colocar a los usuarios en las listas de denegación de servicio y vigilancia según corresponda, y

13.3.3 Información sobre el CDD y revisiones de documentos (tanto espontaneas como periódicas).

13.4 Además de las revisiones de CCD, la Compañía se involucrará en actividades de monitoreo de transacciones. La Compañía participará en el análisis de los patrones de transacciones de los clientes a través del análisis de datos y herramientas de detección de actividad sospechosa para evaluar si las transacciones particulares están fuera de las tendencias generales/perfil de riesgo que la Compañía ha establecido (agregando transferencias por múltiples puntos de datos) y/o el enfoque típico adoptado por los clientes específicos.

13.5 Cuando una transacción se presente como potencialmente de un mayor riesgo de delito financiero basado en el monitoreo anterior, la Compañía llevará a cabo investigaciones adicionales apropiadas para determinar si hay delito financiero presente, o motivos de sospecha de delitos financieros. Esto puede dar lugar a un informe al CO.

13.6 Para mitigar aún más los riesgos, la Compañía impone umbrales de valor de transacción por los que los clientes que deseen realizar intercambios de mayor valor deben estar sujetos a mayores niveles de CDD para reflejar el mayor riesgo de delincuencia financiera. Dichos umbrales funcionan con evaluaciones de transacciones acumulativas e individuales para disminuir la probabilidad de smurfing permitiendo que las transacciones/clientes eviten CDD adicional.

14. MANTENIMIENTO DE REGISTROS

14.1 Existen requisitos mínimos de mantenimiento de registros para el CDD llevada a cabo para fines de AML. La Compañía debe llevar registros de cualquier documento que haya obtenido como parte de la CDD que ha llevado a cabo a los clientes durante 5 años, comenzando en la fecha en que tiene motivos razonables para creer que la transacción o relación comercial ha llegado a su fin - Consulte la política de retención de la Compañía para obtener más información.

15. FORMACIÓN DEL PERSONAL

15.1 La Compañía lleva a cabo capacitación específica sobre AML, CTF y delitos financieros como parte de su proceso de incorporación de empleados, y es obligatorio que todos los empleados lleven a cabo capacitación de actualización sobre estos temas de manera continua.

15.2 El programa de formación es responsabilidad del CO que, con el asesoramiento y el apoyo externos adecuados, garantiza lo siguiente:

Contenido	- Régimen legal y reglamentario del Reino Unido en relación con el crimen financiero. - Las infracciones específicas que pueden ser cometidas por varios empleados dentro de la empresa. - El papel del CO.

	- El delito financiero corre el riesgo de que el negocio esté expuesto y cómo la Compañía busca mitigarlos y manejarlos. - Los procedimientos CDD y SAR que la Compañía tiene en vigencia, así como obligaciones más amplias de los empleados con respecto a la lucha contra los delitos financieros.
Destinatarios	- Todos los directores, altos directivos y empleados - Los consultores, secondes y trabajadores similares se determinarán caso por caso
Frecuencia	- Todos los empleados recibirán capacitación como parte de su incorporación como empleados. - En un punto definido anualmente, todos los empleados completarán una sesión de capacitación de actualización.
Método de entrega	- Diapositivas de capacitación basadas en escritorio, accesibles a discreción de los empleados
Confirmación	- Cada vez que un empleado reciba capacitación, se le pedirá que complete una evaluación obligatoria. Deben aprobar esta evaluación para completar la formación. - Como parte de la revisión anual del desempeño de un individuo, se confirmará si la persona completó la capacitación sobre delitos financieros de ese año. Además, los sistemas automatizados identificarán al CO aquellos que no hayan completado la formación anual en el plazo de 1 mes a partir de la vida del programa de formación.

16. PROCEDIMIENTOS PARA TRATAR CON SOLICITUDES RELACIONADAS CON AML SOBRE LA COMPAÑÍA DE OTRAS PARTES

16.1 Algunos proveedores de servicios profesionales a la Compañía (en particular bancos y otras instituciones financieras, abogados y agentes) estarán bajo las obligaciones de AML de llevar a cabo "conocer a su cliente" ('KYC', por sus siglas en inglés) en la Compañía como su cliente. La obligación clave que les imponen los MLRs 2017 es confirmar y verificar la identidad de su cliente y, por lo general, deben hacerlo antes de que puedan prestar sus servicios. Del mismo modo, de vez en cuando, las empresas de servicios profesionales que actúen para otras partes (por ejemplo, los abogados que actúen para un inversionista) estarán obligadas a llevar a cabo KYC en la Compañía como una de las otras partes en los acuerdos (por ejemplo, cuando la plataforma se utiliza para comprar inversiones emitidas por una entidad y la Compañía remite los fondos de finalización a la entidad).

16.2 Si bien una búsqueda de Companies House permitirá a terceros identificar y verificar información clave como el nombre de la Compañía, el número de registro y la dirección del domicilio social, los MLRs 2017 requieren que las empresas tomen un enfoque basado en el riesgo. Esto significa que la Compañía puede recibir solicitudes de información adicional más allá de lo contenido en los registros públicos, particularmente cuando la transacción que genera el requisito de llevar a cabo KYC en la Compañía presenta indicadores de que hay una riesgo de lavado de dinero.

Cuando esto ocurre, los empleados de la Compañía deben pedir a la persona que hace la solicitud que explique y justifique la base de la solicitud, y luego las solicitudes deben considerarse caso por caso.

PROCEDIMIENTOS KYC

Este procedimiento describe el proceso por el cual la Compañía lleva a cabo la debida diligencia del cliente en los potenciales clientes/comerciantes antes de que se les dé acceso a los servicios. El mismo procedimiento se utiliza para cuando un cliente existente cambia su relación con la Compañía (por ejemplo, si comienza a participar en una gama más amplia de criptomonedas, o coloca significativamente más fondos en la plataforma). El propósito de este procedimiento es ayudar a la Compañía a desarrollar negocios que estén dentro de su apetito por el riesgo comercial, pero también asegurarse de que cumpla con sus obligaciones con respecto a la debida diligencia del cliente que surgen bajo la legislación británica contra el lavado de dinero y evita que sus servicios se utilicen para los fines de otros delitos financieros.

1. PASO 1 – IDENTIFICAR AL CLIENTE Y DEFINIR EL CASO DE NEGOCIO

Esta etapa es muy importante, ya que sienta las bases sobre las que se basará el procedimiento KYC. El proceso seguido variará dependiendo de cómo el cliente va a utilizar la plataforma.

Comerciantes

1.1 Esta etapa consiste en recopilar tanta información como sea posible del comerciante y revisarla para comprender completamente la propuesta de negocio del cliente.

1.2 Durante esta etapa, la información recopilada del cliente debe abordar las siguientes preguntas:

1.2.1 ¿En qué país está registrado el comerciante y cuál es el nombre del comerciante? ¿Quiénes son los directores, altos directivos, accionistas, etc.?

1.2.2 ¿Qué divisas les gustaría recibir la liquidación de su balance?

1.2.3 ¿Dónde está la cuenta bancaria del comerciante (qué banco y en qué país)?

1.2.4 ¿Qué están vendiendo? ¿Cuál es el producto/servicio y a qué industria pertenece? ¿Quiénes son sus clientes típicos?

1.2.5 ¿Cuáles son sus mercados objetivo/regiones principales de donde provienen los clientes?

1.2.6 ¿Necesitan una licencia para operar? ¿Hay una licencia? En caso afirmativo, ¿quién lo emitió y cuándo?

1.2.7 ¿Durante cuánto tiempo han estado activos?

1.2.8 ¿Alguna información adicional que debamos tener?

1.3 Esta etapa debe estar bien documentada internamente para cumplir con, y dar pruebas de dicho cumplimiento, con los requisitos de AML del Reino Unido, así como la identificación del riesgo de que el cliente potencial puede utilizar la plataforma con fines fraudulentos. Las respuestas a estas preguntas deben ser documentadas e ingresadas en los registros de la Compañía sobre el cliente potencial.

Cliente Comprador

1.4 Esta etapa consiste en reunir tanta información como sea apropiado y posible del cliente para que la Compañía tenga claro quién es el cliente, y para que esto pueda ser verificado con evidencia documental.

1.5 Durante esta etapa, la información recopilada del cliente debe abordar las siguientes preguntas:

1.5.1 ¿Quién es el cliente real (es decir, particular, empresa, fideicomiso, etc.)? ¿Cuál es la relación de la persona que completa la información de identificación con la entidad?

1.5.2 Si la entidad es una empresa, ¿en qué país está registrada la empresa y cuál es el nombre de la empresa? ¿Quiénes son los directores, altos directivos, accionistas, etc.?

1.5.3 Si la entidad es una persona, ¿cuál es su nombre, cuál es su fecha de nacimiento y dónde residen?

1.5.4 Si es un fideicomiso, ¿quiénes son los beneficiarios, los fideicomisarios, etc.?

1.5.5 ¿Qué criptoactivos tienen la intención de intercambiar?

1.5.6 ¿Qué volumen de transacciones tienen intención de llevar a cabo?

1.5.7 ¿Qué comerciantes tienen la intención de usar?

1.5.8 ¿Alguna información adicional que debamos tener?

1.6 Esta etapa debe estar bien documentada internamente para cumplir con, y dar pruebas del cumplimiento, con los requisitos de AML del Reino Unido, así como la identificación del riesgo de que el cliente potencial puede utilizar la plataforma con fines fraudulentos. Las respuestas a estas preguntas deben ser documentadas e ingresadas en los registros de la Compañía sobre el cliente potencial.

2. PASO 2 – RECOLECCIÓN DE DOCUMENTOS

2.1 Cada cliente (independientemente de cómo utilizará los servicios), si es una entidad constituida, deberá proporcionar los siguientes documentos para su revisión:

2.1.1 Certificado de constitución

2.1.2 Memorando y artículos de asociación

2.1.3 Identidades de Propietarios Beneficiarios (que pueden estar sujetos a CDD como si fueran el cliente directo, en función de su perfil de riesgo)

2.1.4 Identidades de los directores (o equivalentes) (que pueden estar sujetos a CDD como si fueran el cliente directo, en función de su perfil de riesgo).

Estos documentos deben estar certificados por un abogado, contador, notario público o funcionario consular de la Embajada o Consulado Británico.

Comerciantes

2.2 Además de los documentos especificados en el párrafo 2.1la Compañía requerirá documentos emitidos por un tercero regulado que proporcione una prueba de dirección comercial (por ejemplo, facturas de servicios públicos para la propiedad / extractos de los registros de la compañía).

2.3 La Compañía también requiere que todos los comerciantes, socios y cualquier Propietario sin fines beneficiarios de un comerciante (según corresponda) y, cuando el comerciante sea una empresa constituida, al menos dos directores del comerciante proporcionen pruebas de verificación que cumplan cada una de las categorías detalladas en la tabla en el párrafo 2.4

Cliente Comprador (y propietarios/directores beneficiarios cuando proceda)

2.4 Se adopta un enfoque de proporcionalidad del riesgo para la verificación de los clientes compradores. Dependiendo del volumen de transacciones que pretendan o estén llevando a cabo, se pueden realizar niveles adicionales de verificación. En la tabla siguiente se muestra cómo se implementa:

Verificación requerida	Los clientes a los que se aplica	Evidencia aceptada	Método de recolección
Nombre y fecha de nacimiento	Todos los clientes	Documento de identidad (por ejemplo, copias en color del pasaporte)	Fotografía tomada por el cliente
Comprobante de residencia	• Clientes que tengan la intención o han superado $100 en transacciones diarias en cualquier día. • Clientes que tengan la intención o hayan superado los $1,000 en transacciones mensuales en cualquier mes. • Clientes que presentan un riesgo de delito financiero moderado	Facturas de servicios públicos o documentos similares (no más de 3 meses).	Fotografía tomada por el cliente
Datos biométricos	• Clientes que tengan la intención o han superado $1,000 en transacciones diarias en cualquier día. • Clientes que tengan la intención o hayan superado los $5,000 en transacciones mensuales en cualquier mes. • Clientes que presentan un mayor riesgo de delito financiero	Imagen del cliente	Exploración fotográfica y facial capturada a través del dispositivo del cliente utilizando la aplicación de la Compañía

2.5 Como se detalló anteriormente, dependiendo del nivel particular de las transacciones que un cliente de realiza, estarán sujetos a niveles adicionales de CDD debido al aumento del riesgo de delito financiero que representan mayores volúmenes de transacciones. Los sistemas de la Compañía monitorean automáticamente los volúmenes de transacciones de un cliente de forma continua. Cuando un cliente alcanza el límite de valor de transacción de su nivel de verificación actual, los sistemas de la Compañía suspenderán inmediatamente la capacidad de ese cliente para realizar más transacciones hasta que completen los requisitos para el siguiente nivel de Verificación. El cliente recibirá una notificación avisándole de la necesidad de enviar información adicional sobre CDD y las implicaciones de no hacerlo. Tras el envío por parte del cliente de los

datos solicitados adicionales, y la Compañía confirmando que cumple con sus requisitos para el CDD adicional, se restablecerá la funcionalidad del cliente.

3. REVISIÓN

3.1 Durante la revisión de la información de verificación, un miembro del equipo de cumplimiento:

3.1.1 revisará de la adecuación de las pruebas documentales recibidas;

3.1.2 comparará la documentación recibida con la información recopilada del cliente; y

3.1.3 obtendrá un informe que incluye chequeos de personas políticamente expuestas ("PEP") y chequeos de sanciones y cualquier otra persona relevante nombrada como parte de la recopilación de información.

3.2 Cualquier discrepancia se resalta y se pone de en conocimiento del CO. Dicha acción puede dar lugar a:

3.2.1 La identificación de un posible riesgo de blanqueo de dinero/delito financiero y subsecuente activación de los procesos de notificación pertinentes;

3.2.2 identificación de que se requiere un CDD reforzado o información adicional sobre el cliente, en cuyo caso se contratará al CO y se buscará asesoramiento sobre los pasos adicionales de verificación que deben emprenderse; o

3.2.3 que la documentación e información actual se considere adecuada, y por lo tanto se continuará el proceso estándar de CDD.

3.3 Además, cualquier documentación faltante o que no se ajuste a los estándares de la Compañía es motivo de rechazo de la solicitud.

3.4 Como parte del proceso descrito en el párrafo 3.1anterior, se realizarán las siguientes comprobaciones:

Comprobación de autenticación de documentos y comprobación de lista de PEP/sancionación

3.5 Los miembros del personal responsables de realizar CDD en cualquier tipo de cliente deberán, en todos los casos, ingresar detalles sobre:

3.5.1 su identidad (por ejemplo, nombre completo, fecha de nacimiento, dirección); y

3.5.2 documentos reunidos con fines de verificación (por ejemplo, número de pasaporte),

en la plataforma integrada proporcionada por el proveedor de servicios externo que la Compañía utiliza para ayudar con acciones adicionales de identificación/verificación.

3.6 Cuando esta plataforma devuelve un resultado que indica:

3.6.1 uno o más de los documentos que el cliente ha proporcionado son, o pueden ser, falsos, inexactos y/o incompletos; y/o

3.6.2 el cliente aparece en una lista de PEP/sanción,

El miembro del personal debe:

3.6.3 revisar los resultados para confirmar si se trata de un resultado falso positivo claro o si hubo un defecto en los datos iniciales que el miembro del personal aportó;

3.6.4 3.2

Comprobación reputacional

3.7 Los controles de Google se realizan en todas las empresas e individuos que aparecen en los documentos de la empresa, así como en el sitio web. Palabras clave se utilizan para encontrar resultados negativos como estafa, fraude, etc.

3.8 Durante esta comprobación, el revisor debe considerar:

3.8.1 Para los comerciantes - cuánto tiempo ha estado en existencia la marca o empresa (y verificar que no se encuentran resultados de antes de estas fechas) y si hay una indicación de participación PEP. Además, también se considerarán medios adversos de cualquier tipo.

3.8.2 Para los clientes compradores/propietarios/directores beneficiarios – si hay alguna indicación de que el cliente está o puede estar involucrado con PEP. Además, también se considerarán medios adversos de cualquier tipo.

3.9 Los resultados negativos encontrados se intensifican y se toma una decisión si esto impide que la Compañía abordo al cliente y/o si necesita ser discutido con el cliente.

4. REVISIÓN Y APROBACIÓN

4.1 Es política de la Compañía no proporcionar acceso a los servicios, aceptar activos de, o llevar a cabo cualquier transacción de cualquier tipo con respecto a, cualquier cliente hasta que (i) ese cliente ha proporcionado documentación cumpliendo con los estándares establecidos anteriormente, (ii) la identidad del cliente ha sido verificada a un nivel adecuado de acuerdo con su perfil de riesgo, y (iii) el cliente ha aceptado los términos de negocio relevantes establecidos anteriormente.

4.2 En el caso de que el proceso KYC descrito anteriormente se lleve a cabo como KYC repetido para un cliente existente (por ejemplo, porque ha surgido una sospecha durante el curso de una relación, o porque la información ha salido a la luz de que el perfil de riesgo original del cliente ha cambiado), y el cliente no es capaz de proporcionar documentación que cumpla con el estándar requerido, la Compañía terminará su relación comercial existente y considerar si se requiere una divulgación a las autoridades del Reino Unido.