Sobre Criptoactivos y Controles

En anteriores entregas, ya hemos hablado de los enfoques empleados en distintas jurisdicciones frente al tratamiento de los activos virtuales. A la fecha, la adopción más popular es un enfoque basado en riesgo que impone requisitos a los proveedores de activos virtuales similares a los impuestos sobre el sector financiero (debida diligencia, licencia para operación, contabilidad, reportes de operación sospechosa). La completa prohibición de activos virtuales también ha mostrado ser una opción latente con menos dolores de cabeza para los reguladores.

Idealmente, un proveedor de activos virtuales debería aplicar todas las medidas preventivas contenidas en la Recomendaciones 9 a 21 dictadas por el GAFI. Lo mismo aplica para entidades financieras y no financieras que se vean envueltas en este mercado. A continuación se revisan algunos de los elementos menos obvios de dichas recomendaciones:

Transacciones Ocasionales
Además de aplicar la Debida Diligencia (DD) a todos los clientes habituales, también se requiere para aquellos ocasionales que transen montos en activos virtuales superiores a los 1000 Euros o Dólares en efectivo o mediante transferencias, donde haya sospecha de lavado de dinero o donde se presuma datos de identificación falsos. Por supuesto, el criterio de "ocasional" deberá ser determinado por cada entidad.

Información de identificación y verificación
Usualmente se emplean identificadores como dirección física, fecha de nacimiento, número de identificación oficial, entre otros. No obstante, en este contexto urge la necesidad de información adicional que puede ir desde dirección IP con una marca de tiempo asociada, geolocalización, información del dispositivo, direcciones de billeteras virtuales, *hash.*

Es altamente recomendable, pensar en opciones de identificación digital que cumplan con los criterios de independencia y confiabilidad propuestos por el GAFI en su guía sobre el uso de identidad digital.

Perfiles de Riesgo
Se debe construir un perfil a partir de la información obtenida para dirigir el enfoque basado en riesgo (mayor, menor escrutinio de transacciones o fin de la relación). A nivel de cliente es posible considerar la naturaleza y volumen de la actividad comercial, origen de activos virtuales depositados o bien, a nivel de segmento; clientes con volumen transaccional similar empleando un activo virtual específico. De cualquier forma, la actualización de estos perfiles debe ser periódica.

Listas Negras
Debe tenerse presente que OFAC ya ha incluido direcciones de monedas digitales en la lista SDN. Esto significa un nuevo campo a considerar al momento de cruzar información, asignándole una importancia similar a la coincidencia con nombres. Además, los sujetos obligados podrían generar y compartir sus propias listas, por ejemplo, cuando algún participante se niegue a continuar operando por los requisitos de debida diligencia solicitados.

Mantenimiento Registros
Los sujetos obligados deberán mantener registros de las operaciones e información de debida diligencia hasta por 5 años. Aquí, la información referente a la identificación de clientes y beneficiarios adquiere una importancia mayor en comparación al mercado financiero tradicional. No basta con conservar las claves públicas[1], direcciones o cuentas involucradas, no basta fiarse solo de los registros blockchain. Si bien, las autoridades pueden eventualmente rastrear transacciones hasta una billetera puntual puede que no se logre asociar fácilmente a una persona natural, por tal motivo es que la información adicional que conserven los proveedores de activos virtuales es necesaria para la vinculación con una persona real.

Licencias
Países como Estados Unidos, Reino Unido y México poseen un marco legal que obliga licencias de operación para los participantes en el mercado de activos virtuales. Lógicamente además de aplicar para obtener el permiso, los sujetos obligados deberían verificar si su contraparte que envía o recibe cuenta con licencia de operación.

Transmisión de Información

Los sujetos obligados en este mercado deben obtener, mantener y transmitir la información asociada a su contraparte sobre el originador y beneficiario de la transacción; así como abstenerse de procesar operaciones con información incompleta.

Aunque el GAFI es tecnológicamente neutral presenta algunas tecnologías útiles al momento de conducir este requerimiento en tiempo real; se basan en el uso de las claves públicas y privadas propias de la criptografía: Conexiones SSL/TLS; Certificados X.509; API, entre otros.

Se escapan muchas aristas en el sistema de prevención que deben aplicar las partes obligadas, como la identificación y tratamiento de PEPs, el grado de debida diligencia aplicable, el monitoreo continuo, entre otros. Hemos decidido dejarlos de lado porque son los que mayor similitud tienen con el mercado financiero tradicional, resaltando en todo momento que no son menos importantes.

En criptoactivos podemos entender la clave pública como un tipo de cuenta bancaria, que se usa para recibir monedas. Mientras que la clave privada se emplea para firmar y enviar monedas.