Manual Guía No. 25

Recomendaciones para la identificación y prevención de esquemas de defraudación

XX de mes de 2021

amv

Autorregulador del Mercado de Valores de Colombia

Tabla de contenido

Versión para comentarios

1. Introducción

La prevención de los esquemas de defraudación a los cuales se enfrentan los Intermediarios del Mercado de Valores (IMV) e Intermediarios del Mercado Cambiario (IMC) tiene un efecto directo sobre la confianza de los inversionistas y la solidez de los mercados. Al respecto, autoridades alrededor del mundo hacen un llamado a los participantes del mercado para prestar especial atención a la identificación y prevención de este tipo de esquemas.

En particular, la Organización Internacional de Comisiones de Valores (IOSCO)[1] señala que las condiciones de operación derivadas de la pandemia[2] y el uso de nuevas herramientas tecnológicas podrían propiciar escenarios para la materialización de los riesgos asociados a dichos esquemas, lo cual afecta no solamente los recursos económicos de los inversionistas, sino también los recursos de los propios IMV. Adicionalmente, IOSCO resalta que el intercambio de información entre las autoridades y participantes del mercado sobre los tipos de fraude detectados y los elementos que los estafadores utilizan coadyuvan a sensibilizar a los inversionistas y a los propios intermediarios del mercado acerca de la manera de operación de esos esquemas fraudulentos[3].

Asimismo, IOSCO y otras autoridades alrededor del mundo han alertado a los intermediarios y a sus clientes sobre el incremento de denuncias de casos de fraude cometidos por agentes externos a las entidades. Al respecto, a nivel global se observa un aumento de la participación de los inversionistas *retail* en los mercados de valores[4], quienes pueden ser más propensos a ser víctimas de dichos esquemas[5].

AMV y sus Comités de Control Interno y Compliance, Renta Variable, Renta Fija y Divisas revisaron diferentes esquemas de defraudación, enfocándose en los elementos de aquellos que potencialmente afectan a los intermediarios y sus personas naturales vinculadas (PNV). Asimismo, se revisaron experiencias de autoridades en otras jurisdicciones las cuales han emitido alertas sobre las variaciones de esquemas defraudatorios, así como recomendaciones para prevenir su materialización. Con base en lo anterior, el presente manual/guía recoge las principales características de los esquemas de defraudación analizados con el fin de contribuir a su prevención, brindar elementos que permitan a las entidades fortalecer sus mecanismos de control, promover la transparencia e integridad del mercado y fomentar la protección a los inversionistas.

Versión para comentarios

[1] IOSCO es el organismo internacional que reúne a los reguladores de valores del mundo. En la totalidad de sus miembros, se encuentran más del 95% de los mercados de valores globales en más de 115 jurisdicciones. IOSCO desarrolla, implementa y promueve el cumplimiento de estándares reconocidos internacionalmente para la regulación de valores.

[2] La pandemia obligó a las entidades a trasladar su operación a sitios no habituales de trabajo (i.e: hogares de los colaboradores) por lo cual se presentaron una serie de cambios y retos operativos y tecnológicos al interior de cada intermediario para afrontar esta situación y garantizar la operación del mercado.

[3] IOSCO (2020). *Risk Outlook 2021*.

[4] Particularmente, en el mercado local, la Bolsa de Valores de Colombia (BVC) reportó un aumento del 10% al 15% entre 2019 y 2020 de la participación de personas naturales sobre la negociación total de acciones. Ver: Valora Analitk "Personas naturales ya negocian 15 % del monto total de acciones en Bolsa de Colombia"

[5] IOSCO (2020). *Retail Market Conduct Task Force Report Initial Findings and Observations About the Impact of COVID-19 on Retail Market Conduct*.

Este documento se divide en cuatro secciones, incluida esta introducción. La segunda y tercera sección desarrollan situaciones de defraudación realizadas por personas externas e internas a la entidad, respectivamente, y presentan recomendaciones asociadas a su prevención. Finalmente, se concluye e incluye un anexo de casos locales sancionados por defraudación.

2. Esquemas de defraudación externos

Los esquemas de defraudación externos se caracterizan porque los actos de fraude son realizados por una persona externa a la organización, que busca apropiarse indebidamente de activos de los clientes de la entidad.

A continuación, se presentan algunas situaciones de defraudación cometidas por externos y recomendaciones para su prevención.

2.1 Suplantación de la identidad del cliente

El esquema defraudatorio implica circunstancias como:

a) Se realiza a través de mecanismos de comunicación impersonal (i.e: call center, correo electrónico).
b) El suplantador solicita el cambio de datos de la cuenta del titular, tales como dirección, teléfonos, correos electrónicos y cuentas bancarias a las cuales se debe desembolsar el dinero producto de la venta de valores. Estas cuentas pueden tratarse de cuentas bancarias "fraudulentas" usando la identidad del cliente[6] o de terceros. En este sentido, se ha identificado un mayor riesgo de suplantación a través de la apertura de cuentas 100% virtual (i.e: Cuentas de Ahorro de Trámite Simplificado-CATS, cuentas de inversión en aplicaciones móviles), al no requerir un contacto directo con la entidad.
c) El suplantador solicita la transferencia de pequeñas cantidades de dinero con el fin de no generar alertas.

Una variación de esta modalidad consiste en que el defraudador obtiene un duplicado de la *SIM CARD* del cliente. De esta manera, a través del "secuestro" de la línea móvil de la persona logra el acceso a los elementos de autenticación ante la entidad que le permiten el ingreso a portales y la modificación de datos. Adicionalmente, la suplantación se puede presentar cuando el defraudador obtiene acceso a los correos electrónicos registrados por los clientes o crea un correo espejo a través del cual envía instrucciones de operaciones.

Finalmente, se ha detectado que, en algunos casos, el suplantador crea correos electrónicos muy similares a los e-mails corporativos de los clientes de los intermediarios. A través de estos

[6] La Autoridad Reguladora de la Industria Financiera (FINRA) y otros organismos internacionales señalan que los suplantadores han aprovechado la implementación de nuevas plataformas tecnológicas que permiten realizar la apertura de cuentas en línea para crear cuentas falsas a nombre del cliente a las cuales desvían los recursos que estos tienen depositados en los intermediarios. Ver: FINRA (2020) *Regulatory Notice 20-13. Heightened Threat of Fraud and Scams*.

Versión para comentarios

correos, el defraudador se hace pasar por los directivos o por las personas autorizadas para realizar operaciones y/o transferencias y solicita el giro de fondos[7].

2.2 Suplantación de la identidad del intermediario

En este esquema, el estafador se comunica con el cliente y se hace pasar por el intermediario con el objetivo de que el cliente le entregue su información personal, lo que le permite, posteriormente, realizar operaciones o transacciones para trasladar los recursos del cliente a otras cuentas.

De acuerdo con algunas autoridades[8], la probabilidad de ocurrencia de este tipo de esquemas es más frecuente en clientes que no tienen mucho contacto con las entidades o en aquellos que no tienen un conocimiento adecuado sobre los productos que pueden ofrecer los intermediarios o de los cobros que estos realizan.

Para el desarrollo de estos esquemas el defraudador utiliza diferentes herramientas que se caracterizan por: la creación de páginas de internet que suplantan al intermediario (*pharming*); el envío de correos electrónicos fraudulentos supuestamente remitidos por la entidad en los cuales se solicita la información personal del cliente (*phishing*); la remisión de mensajes de texto que solicitan a los clientes actualizar o remitir información privada (*smishing*); o llamadas telefónicas que suplantan a la entidad (*vishing*).

Por otro lado, se ha identificado defraudadores que se hacen pasar por un funcionario de la entidad que se comunica con la mesa de ayuda (IT, help desk), o viceversa, para intentar obtener información sobre la entidad y/o los clientes, y con ello cometer el fraude[9].

2.3 Recomendaciones para la prevención de esquemas de defraudación externos

a) Implementar señales que faciliten la detección de esquemas fraudulentos. En especial se recomienda evaluar la incorporación de alertas sobre las solicitudes de los clientes que contengan alguno de los siguientes elementos:
   i. lleguen a una hora inusual del día;
   ii. utilicen un lenguaje o saludos atípicos;
   iii. soliciten una transferencia a una nueva cuenta, el giro de recursos a terceros o aspectos en la modificación de las cuentas bancarias que llamen la atención

[7] El FBI señaló un caso en el cual unos estafadores enviaron un correo electrónico a una institución financiera, suplantando al director general de una empresa que era cliente de la entidad, y que había programado previamente una transferencia de USD $1 millón. En el correo se solicitaba adelantar la fecha de la transferencia y cambiar la cuenta del destinatario. El correo utilizado por los estafadores era casi idéntico a la cuenta real del director de la empresa. Ver: *FBI National Press Office*

[8] En octubre de 2020, FINRA advirtió sobre la suplantación de su identidad por medio un email remitido desde el dominio "@regulation-finra.org" y a través del cual se solicitaba a los destinarios sus datos personales e información sobre sus productos financieros. Adicionalmente, FINRA alertó sobre la existencia de sitios web falsos que se hacen pasar por corredores de bolsa autorizados. Asimismo, en Canadá, la Organización Reguladora de la Industria de Inversión (IIROC) ha advertido sobre la vulnerabilidad de los clientes que, en algunos casos, no son conscientes que son víctimas de un fraude.

[9] FINRA (2020) Regulatory Notice 20-13. Heightened Threat of Fraud and Scams. FINRA ha indicado que las empresas abordan los riesgos relacionados con estos mecanismos capacitando al personal del servicio de asistencia para que verifique la identidad de las personas que se comunican con ellos.

Versión para comentarios

(i.e: una corta vigencia de creación o que hayan sido abiertas en una ciudad distinta de la del domicilio del cliente).

iv. exijan privacidad o secreto para la ejecución de las transacciones;
v. cambios de última hora en las instrucciones de la transferencia o en la información de la cuenta del destinatario;
vi. muestren una urgencia inusual, por ejemplo, solicitar operaciones de manera inmediata a la actualización de información;
vii. el cliente desconoce o no recuerda información sobre su portafolio o su cuenta;
viii. quejas recurrentes de los clientes por extractos no recibidos o información incorrecta de estos[10].

b) Verificar la identidad del cliente antes de ejecutar cualquier solicitud para la realización de operaciones o transferencias. En particular, sobre aquellas transacciones enviadas a través del correo electrónico. Por otra parte, se recomienda sospechar ante la negativa inusual del cliente de comunicarse por teléfono o plataformas de voz o vídeo en línea.
c) Verificar que la dirección de correo electrónico del remitente coincida con la registrada por el cliente y estar atentos a los hipervínculos que puedan contener errores ortográficos o variaciones de la cuenta real.
d) Establecer procedimientos de vinculación de los clientes y mecanismos robustos tipo "Conozca a su Cliente", que le permitan al intermediario asegurar que la persona que interactúa con la entidad corresponde efectivamente al titular. Antes de brindarle al cliente alguna información respecto de su cuenta o portafolio es recomendable ejecutar los procedimientos de verificación de la identidad del cliente. Lo anterior, por cuanto se ha observado que el defraudador utiliza la información que el propio intermediario le suministra para posteriormente cometer el fraude.
e) Contar con procedimientos de verificación, validación y consulta de información adicional de los clientes, como por ejemplo la información financiera en centrales de riesgo con el objetivo de corroborar la veracidad de la información que es entregada por el cliente.
f) Confirmar con el cliente la actualización de su información a los teléfonos registrados en los formularios de vinculación. Asimismo, implementar tarjetas de firmas (digitales o físicas) que permitan confrontar la identidad de quien envía la comunicación de autorización de venta u otros trámites.
g) Implementar controles adicionales a los tradicionales maker/checker, con varios niveles de revisión y mecanismos de vigilancia adicionales complementarios a los controles duales.
h) Fortalecer las estrategias de cultura y seguridad, y las campañas de educación financiera dirigidas a los clientes, por medio de las cuales son advertidos sobre las modalidades de defraudación. De esta manera, los clientes pueden actuar como

[10] Por ejemplo, si los clientes manifiestan discrepancias en su cuenta, transacciones no autorizadas, dinero faltante u otros problemas en sus estados de cuenta, se podría estar frente una situación de fraude. Asimismo, implementar procesos para investigar y responder rápidamente a las quejas, llamadas y consultas de los clientes ante dichas situaciones.

Versión para Comentarios

primera línea de defensa para la detección este tipo de esquemas y contribuir a su prevención.

i) Generar el bloqueo preventivo de las operaciones o productos de los clientes en casos de alertas sobre posible fraude.
j) Denunciar ante las autoridades competentes y/o de mercado (ie: Fiscalía General de la Nación, Superintendencia Financiera de Colombia, AMV) las situaciones de fraude identificadas. Adicionalmente, notificar a las entidades financieras donde se originaron las cuentas de ahorro o corriente fraudulentas detectadas.
k) Utilizar nuevas herramientas tecnológicas y de análisis de datos como *big data* o *machine learning* para generar alertas basadas en el comportamiento transaccional de los clientes.
l) Crear notificaciones dirigidas a los clientes para informar: cambios en la información de las cuentas bancarias registradas, la actualización de datos personales o la recepción o trámite de instrucciones ya sea por correo electrónico, mensaje de texto o mensajes instantáneos. Asimismo, informar en dichas comunicaciones los medios de contacto oficiales que la entidad tiene disponibles.
m) Solicitar al cliente el cambio de contraseñas en los portales web de cada entidad de manera periódica. Adicionalmente, establecer contraseñas estructuradas que incluyan parámetros alfanúmeros o caracteres especiales.

3. Esquemas de defraudación internos

Esta categoría está relacionada con los actos realizados por un colaborador de la entidad, que tienen como objetivo apropiarse indebidamente ya sea de los activos de la entidad y/o de sus clientes.

En el Reglamento de AMV la defraudación es considerada un abuso de mercado e involucra tres elementos, a saber: i) obtener provecho indebido para sí o para un tercero; ii) afectar a un tercero o al mercado; y iii) ejecutarse en desarrollo de operaciones o actividades de intermediación[11].

A continuación, se describen algunas conductas que pueden ser asociadas a esquemas de defraudación interna y, posteriormente, se indican recomendaciones para su prevención.

3.1 Conductas asociadas a la defraudación interna

Los siguientes son elementos y conductas identificados en la ejecución de esquemas de defraudación internos:

a) Los recursos de los clientes se transfieren o destinan a cuentas que no han sido autorizadas por ellos. Para ello, el defraudador utiliza; i) la creación de instrucciones falsas por medio de las cuales ordena el traslado de recursos a cuentas de terceros; ii) la alteración de órdenes de transferencia impartidas por los clientes donde se

[11] Reglamento de AMV. Artículo 49.1 Defraudación

Versión para comentarios

modifica el beneficiario o portafolio al que se deben transferir recursos; y iii) la suplantación de los clientes para dar instrucciones sobre sus portafolios.

b) Los títulos de los clientes son utilizados en operaciones que no han sido autorizadas por estos.
c) El suministro de información incorrecta a los clientes sobre sus inversiones con el fin de evitar la detección de los actos fraudulentos.
d) La realización de operaciones de intermediación, con clientes u otros intermediarios, que tienen el objetivo de generar una utilidad o beneficio indebido para sí o para un tercero.
e) El ofrecimiento de productos que no son administrados por el intermediario.

Caso sancionado por defraudación en el mercado local[12]

Un asesor se apropió de recursos por COP $258,8 millones de 28 clientes de la SCB a la cual se encontraba vinculado. Se identificó que 18 de esos clientes superaban los 60 años y no realizaban movimientos habituales en sus inversiones.

Para la implementación del esquema de defraudación el asesor elaboró, sin la autorización de los clientes, 50 cartas de instrucciones utilizando la firma escaneada de estos. A través de las cartas ordenó destinar los recursos a cuentas bancarias de terceros afectando a los clientes. Adicionalmente, en algunos casos, solicitó la expedición de cheques a nombre de terceros. Aunque las instrucciones de transferencias eran entregadas al área de tesorería de la entidad, debido a que el monto de las transferencias era inferior a los COP $ 50 millones, estas instrucciones no eran sometidas a confirmación telefónica con los clientes.

Igualmente, el asesor que cometió la defraudación suministraba a los clientes afectados información que no correspondía con los saldos reales de sus inversiones en los Fondos de Inversión Colectiva (FIC). Además, se comprobó que parte de los recursos que llegaron a la cuenta de los terceros a las cuales eran solicitadas las transferencias, posteriormente, fueron transferidos a la cuenta bancaria personal del investigado obteniendo provecho indebido para sí o para un tercero.

Con el fin de contribuir a la identificación de los esquemas de defraudación internos, en el Anexo 1 se presentan algunos casos sancionados por el Tribunal Disciplinario de AMV que describen las conductas asociadas.

3.2 Recomendaciones para la prevención de esquemas de defraudación internos

A continuación, se describen recomendaciones que contribuyen en la prevención de los esquemas de defraudación internos:

a) Definir procedimientos para el envío de información a clientes sobre sus movimientos e inversiones, así como, determinar responsabilidades sobre la elaboración y remisión de esta información. De ser posible, implementar mecanismos que permitan hacer seguimiento a la entrega de información a los clientes y restringir la participación en estos procesos a los funcionarios que interactúan de manera directa en la negociación de operaciones con los clientes.

[12] El caso corresponde a la Resolución N°1 del 29 de mayo de 2019 Segunda Instancia y puede ser consultado en el siguiente enlace: https://www.amvcolombia.org.co/profesionales-de-la-industria/sanciones/

Versión para comentarios

b) Contar con una adecuada segregación de las funciones para la ejecución de órdenes de transferencias.
c) Abstenerse de solicitar la suscripción de formatos o documentos en blanco a los clientes.
d) Incorporar avisos hacia los clientes sobre cuál es la única información oficial y cuáles los canales oficiales para su entrega.
e) Diseñar planes de monitoreo aleatorio sobre los correos o comunicaciones enviadas y recibidas de los clientes. Estos pueden incluir: i) la verificación de las líneas telefónicas a través de las cuales los clientes transmiten sus órdenes; y ii) la detección de quejas y reclamos de los clientes que son dirigidas y atendidas directamente por el operador o el asesor financiero.
f) Verificar la respuesta ante las quejas de los clientes por extractos no recibidos o información incorrecta sobre sus recursos.
g) Implementar alertas que permitan prevenir o detectar oportunamente situaciones irregulares, por ejemplo, en relación con: i) los resultados del análisis de la información revelada por las PNV; y ii) cambios significativos en la generación de ingresos o en los gastos incurridos por la entidad.
h) Identificar las operaciones cuyo volumen resulte inusual frente a los valores normales o promedios operados por el funcionario o los clientes.
i) Analizar las operaciones que generen utilidades y/o pérdidas inusuales o que no se ajusten a las estrategias de negocio previamente definidas por la entidad.
j) Observar las operaciones cuyos precios se alejen de las condiciones de mercado o celebradas con títulos cuyos precios de valoración se encuentren rezagados.
k) Establecer mecanismos para analizar la recurrencia de operaciones con las mismas contrapartes y sobre las mismas especies[13]. Asimismo, identificar esquemas de operación recurrente que siempre denoten utilidades o pérdidas con un mismo cliente o contraparte.
l) Monitorear la modificación, anulación y complementación de operaciones con el fin de detectar situaciones irregulares.
m) Implementar buenas prácticas para la protección de clientes con mayor potencial de vulnerabilidad (i.e: Adultos mayores)
n) Notificar al cliente por correo electrónico o celular registrados todos los movimientos realizados en sus cuentas, con el fin de que esté enterado de sus solicitudes y operaciones.
o) Auditar a las áreas que participan en los procesos de solicitud de transferencias o de venta de valores, así como, realizar revisiones no programadas sobre estos procesos con el fin de identificar conductas no apropiadas.
p) Realizar capacitación continua a los funcionarios con el fin de identificar oportunidades de mejora o conductas sospechosas dentro de la organización.
q) En la medida de lo posible, notificar al asesor financiero u operador principal del cliente sobre las solicitudes que este último realiza a otros funcionarios (*backup)* con el fin de validar los procesos a ejecutar por el cliente.
r) Definir procesos especiales de actualización de información o de ejecución de operaciones para aquellos clientes que no tienen un contacto recurrente con el intermediario o no registran actividad en un determinado periodo de tiempo. Lo

[13] Entre las herramientas para contribuir a la detección de posibles abusos de mercado, AMV provee a las entidades diferentes reportes, entre ellos, un informe relacionado con la concentración de contrapartes.

Versión para comentarios

anterior, con el fin de evitar el envío de extractos y notificaciones a direcciones (físicas o electrónicas) que puedan estar desactualizadas.

s) Monitorear las operaciones de clientes sobre las cuales se detecten órdenes incompletas o en las cuales no se defina claramente: el activo a operar, el lado de la operación (compra o venta), el precio o la tasa, el monto y/o no se identifique al ordenante.

4. Conclusión

La prevención de los esquemas de defraudación en los mercados financieros es un elemento clave para fortalecer la confianza de los inversionistas y la solidez de los mercados. Las medidas y controles señalados en este Manual/Guía brindan a los intermediarios de valores y divisas elementos que contribuyen a la mitigación de los riesgos asociados a esquemas defraudatorios como los aquí expuestos.

Versión para comentarios

Anexo 1: Otros casos sancionados por defraudación

Los casos mostrados a continuación han sido sancionados por el Tribunal Disciplinario de AMV y se encuentran publicados en la página web del autorregulador[14].

Caso 1 – Esquema de defraudación entre operadores de diferentes entidades[15]: Los operadores AAA y BBB, que trabajaban en la SCB ABC y en el Banco XYZ respectivamente, ejecutaron 33 operaciones de compra y venta de unos títulos por medio de las cuales generaban unas comisiones para el operador AAA y pérdidas para el Banco XYZ.

Bajo este esquema, el operador AAA compraba o vendía Bonos de Deuda Pública Externa colombiana en dólares a brókeres internacionales, quienes a su vez y de manera inmediata, celebraban una operación de signo contrario con el operador BBB. Posteriormente, BBB negociaba los títulos con AAA. Estas operaciones fueron ejecutadas siempre a un precio que generaba pérdidas para el Banco XYZ y ganancias para SCB ABC.

De esta manera, a través de las comisiones que la SCB ABC pagaba a AAA, este obtuvo beneficios que fueron catalogados como un provecho indebido proporcionales a las pérdidas en las que incurrió el Banco XYZ (afectación a terceros).

Caso 2 – Esquema defraudatorio desviando recursos de los clientes[16]: Un asesor vinculado a la SCB DDD, en el desarrollo de actividades de intermediación, ofreció a siete clientes un producto de inversión que no estaba autorizado por la entidad.

El producto ofrecido supuestamente se basaba en operaciones con CDTs, títulos de renta fija y repos. Los clientes le entregaban al asesor cheques de gerencia a nombre de la SCB DDD para hacer inversiones en dicho producto. Los recursos proporcionados por los clientes alcanzaron los COP $301 millones. Los dineros fueron utilizados por el asesor para cubrir faltantes de otros clientes, obteniendo así un provecho indebido. Esto afectó los recursos de los clientes que creían haber entregado el dinero para realizar determinadas inversiones.

Adicionalmente, el asesor elaboró y suministró a los clientes afectados recibos de caja y certificaciones de inversión que no reflejaban el valor real de sus portafolios.

Caso 3 – Esquema defraudatorio usando títulos de los clientes[17]: Un operador, en el desarrollo de actividades de intermediación, celebró en nombre de sus clientes operaciones sin su autorización sobre títulos de renta fija.

[14] Ver: https://www.amvcolombia.org.co/profesionales-de-la-industria/sanciones/

[15] Tribunal Disciplinario de AMV, Resolución N°17 del 29 de noviembre de 2016 Segunda Instancia y Resolución N°10 del 31 de agosto de 2016 Primera Instancia. Disponible en: https://www.amvcolombia.org.co/2020/sanciones/Resoluciones/Res-17-(01-2015-371)-SR-29-11-2016_Censurado.pdf

[16] Tribunal Disciplinario de AMV, Resolución N°15 del 30 de septiembre de 2016 Segunda Instancia y Resolución N°6 del 31 de mayo de 2016 Primera Instancia. Disponible en: https://www.amvcolombia.org.co/2020/sanciones/Resoluciones/Res-15-(01-2014-362)-SR-30-9-2016_Censurado.pdf

[17] Tribunal Disciplinario de AMV, Resolución N°8 del 11 de agosto de 2016 Segunda Instancia y Resolución N°19 del 10 de diciembre de 2015 Primera Instancia. Disponible en: https://www.amvcolombia.org.co/2020/sanciones/Resoluciones/Res-8-(01-2014-335)-SR-11-8-2016_Censurado.pdf

El operador realizaba la venta y posterior recompra de los títulos de los clientes, en condiciones financieras desfavorables para los inversionistas. A través de este esquema el investigado ejecutó la rotación de un mismo título "por medio de la compra y venta de bonos a tasas consideradas alejadas de las condiciones de mercado entre varios de sus clientes". De esta manera, el vendedor inicial del título terminaba readquiriéndolo a una tasa menor (precio mayor) lo que generó una afectación económica a estos clientes. Tales negocios ocasionaron a los inversionistas pérdidas por COP $73.027.831, utilidades para la compañía de COP $78.273.930 y comisiones de COP $13.068.411, en favor del inculpado.

La celebración de estas operaciones de compra y venta generaron un beneficio económico para el operador vía márgenes y logró de esta manera un provecho indebido.

Caso 4 – Esquema defraudatorio con diferentes modalidades[18]: Un operador vinculado a una SCB, en el desarrollo de actividades de intermediación, direccionó de manera inapropiada recursos entregados por sus clientes por COP $10.110 millones a través de tres modalidades, las cuales se describen a continuación:

i) La suplantación de los clientes en comunicaciones telefónicas por medio de las cuales impartió y ejecutó órdenes para la celebración de operaciones repo y ventas definitivas de títulos. Posteriormente, el operador dirigió, sin la autorización de los clientes, los recursos producto de esas operaciones a terceros, entre los cuales se encontraba la sociedad SSS, de la cual el investigado era socio.

ii) Siete clientes y seis terceros, que no eran clientes de la SCB, consignaron recursos para realizar inversiones en productos que el operador les ofreció. Una vez el operador recibía los comprobantes de consignación o cheques, trasladaba los recursos a cuentas de otros terceros, de tal manera que los recursos no fueron invertidos de acuerdo con las instrucciones de los clientes.

iii) El operador ofreció a los clientes de la SCB una supuesta cartera colectiva denominada "cartera colectiva SSS" que no era administrada por el intermediario. De esta manera, les solicitó a los clientes depositar en una cuenta bancaria a nombre de la sociedad SSS recursos para supuestamente invertir en dicha cartera.

Las diferentes modalidades afectaron los recursos de los clientes engañados, quienes entregaron fondos para realizar inversiones que no existían o se realizaron operaciones que estos no habían autorizado. Adicionalmente, por medio de estos esquemas, el operador se apropió de los recursos de los clientes afectados de manera indebida.

[18] Tribunal Disciplinario de AMV, Resolución N°3 del 9 de noviembre de 2019 Segunda Instancia y Resolución N°3 del 4 de septiembre de 2019 Primera Instancia. Disponible en: https://www.amvcolombia.org.co/wp-content/uploads/2020/05/Segunda-Instancia-Carlos-Suarez.pdf

Bibliografía

AMV – Autorregulador del Mercado de Valores. (2021). *Sanciones.* Recuperado de: https://www.amvcolombia.org.co/profesionales-de-la-industria/sanciones/

AMV – Autorregulador del Mercado de Valores. (2021). *Reglamento de AMV.* Recuperado de: https://www.amvcolombia.org.co/wp-content/uploads/2017/11/Reglamento_AMV-_29-de-diciembre-de-2020.pdf

FIB National Press Office. (2020). *FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic*. Recuperado de: https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

FINRA - Financial Industry Regulatory Authority. (2020). *Regulatory Notice 20-13. Heightened Threat of Fraud and Scams*. Recuperado de: https://www.finra.org/sites/default/files/2020-05/Regulatory-Notice-20-13.pdf

FINRA - Financial Industry Regulatory Authority. (2020). *Regulatory Notice 20-35. Phishing email purporting to be from FINRA*. Recuperado de: https://www.finra.org/sites/default/files/2020-10/Regulatory-Notice-20-35.pdf

IIROC - Investment Industry Regulatory Organization of Canada. *(2020). Notice 20-0235. Cybersecurity and Fraud – Protecting Clients.* Recuperado de: https://www.iiroc.ca/Documents/2020/bbb0160f-2c9c-4b54-85a8-04eb97b94e04_en.pdf#search=20%2D0235

IOSCO - International Organization of Securities Commissions. (2020). *Retail Market Conduct Task Force Report Initial Findings and Observations About the Impact of COVID-19 on Retail Market Conduct. FR13/2020.* Recuperado de: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD669.pdf

IOSCO - International Organization of Securities Commissions. (2020). *Risk Outlook 2021.* Recuperado de: https://www.iosco.org/members_area/file.cfm?file=members-area\documents\pdf\IR01-2020%20Risk%20Outlook%202021.pdf

Valora Analitik. (2021). *Personas naturales ya negocian 15 % del monto total de acciones en Bolsa de Colombia.* Recuperado de: https://www.valoraanalitik.com/2020/12/18/personas-naturales-ya-negocian-15-del-monto-total-de-acciones-en-bolsa-de-colombia/

Versión para comentarios