Naciones Unidas CTOC/COP/WG.2/2024/3

Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

Distr. general
25 de marzo de 2024
Español
Original: inglés

Grupo de Trabajo de Expertos Gubernamentales sobre Asistencia Técnica
Viena, 3 y 4 de junio de 2024
Tema 3 del programa provisional*
Fraude organizado

Fraude organizado

Documento de antecedentes preparado por la Secretaría

Introducción

1. El presente documento de antecedentes ha sido preparado por la secretaría con el fin de facilitar las deliberaciones en relación con el tema 3 del programa provisional de la 15ª reunión del Grupo de Trabajo de Expertos Gubernamentales sobre Asistencia Técnica. Ofrece una sinopsis breve y no exhaustiva de las diferentes categorías de fraude organizado que se utilizan para atacar a personas o instituciones con el fin de obtener un beneficio financiero u otro beneficio de orden material y tiene por objeto promover respuestas más eficaces al fraude organizado, en el marco de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

2. El fraude ha cambiado mucho con los años y se ha adaptado a los avances tecnológicos y a las transformaciones de la sociedad. Se ha vuelto cada vez más sofisticado, utilizando la manipulación psicológica y la tecnología, y recurriendo al aprendizaje automático, la inteligencia artificial y otras tecnologías para automatizar la comisión del delito. El elevado volumen del fraude y su gravedad plantean un riesgo considerable para las personas, para las economías y para la prosperidad en todo el mundo y repercuten negativamente en la confianza pública en el estado de derecho. Sin embargo, elaborar un perfil preciso del fraude presenta varias dificultades. A menudo, las víctimas no lo denuncian suficientemente debido a sentimientos de vergüenza, culpa propia o desconcierto, así como a la falta de reconocimiento de que se ha producido un delito. Además, una parte considerable del fraude va contra las empresas, muchas de las cuales optan por no denunciar estos delitos para evitar dañar su reputación. El anonimato y la lejanía asociados a la comisión de fraudes ocultan aún más la identidad de los delincuentes a las víctimas y a las autoridades, lo que dificulta las gestiones para analizar los patrones subyacentes y los riesgos asociados. Además, la naturaleza dinámica del fraude, que se adapta constantemente a los cambios en los sistemas jurídicos, sociales, comerciales y tecnológicos, hace que los métodos nuevos e innovadores de delincuencia puedan pasar desapercibidos dentro de los datos oficiales estáticos

* CTOC/COP/WG.2/2024/1.

V.24-05658 (S) 150524 150524

3. La comunidad internacional ha reconocido la magnitud preocupante del fraude y la necesidad de aunar esfuerzos para prevenirlo y combatirlo [1]. La Asamblea General, en su resolución 78/229, reafirmó el mandato de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) de prestar cooperación y asistencia técnicas a los Estados Miembros que lo soliciten en relación con todas las formas de delincuencia organizada, incluido el fraude. Esto concuerda con el objetivo de la Convención contra la Delincuencia Organizada, cuyo propósito es promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional, como se articula en su artículo 1. Consciente de la naturaleza cambiante del fraude y del creciente uso de la tecnología para ampliar su alcance, la Asamblea General, en su resolución 74/177, exhortó a los Estados Miembros a que estudiasen medidas y elaborasen posibles conclusiones y recomendaciones destinadas a crear un entorno cibernético seguro y resiliente, prestando especial atención a los delitos relacionados con el robo de identidad.

4. Es un hecho ampliamente reconocido que el fraude puede ser un delito organizado y grave[2]. La evolución de la tecnología, junto con la rápida ampliación del alcance y la magnitud de la delincuencia organizada, han impulsado la creación de una serie de nuevas maneras de estafar a particulares, empresas e incluso Gobiernos a escala masiva y mundial. Esto ha conferido a grupos delictivos organizados la capacidad de atacar con mayor eficacia a sus víctimas en todo el mundo[3].

5. El fraude en el ámbito de la delincuencia organizada posee características bien definidas. En primer lugar, se refiere principalmente al robo de dinero y no a la producción o distribución de bienes ilegales, lo que lo distingue de otras actividades delictivas. En segundo lugar, muchas actividades fraudulentas se llevan a cabo a distancia, facilitadas por una tecnología que permite la comunicación anónima y la transferencia de fondos robados sin interacción física entre el autor del delito y la víctima. En tercer lugar, el fraude suele basarse en que las víctimas faciliten voluntariamente el acceso a sus fondos, y el éxito depende de tácticas engañosas que difuminan las fronteras entre entidades legítimas e ilegítimas. Estos elementos configuran los métodos empleados por los defraudadores, dictan las capacidades necesarias e influyen en la estructura de los grupos delictivos organizados.

6. Algunos de esos defraudadores están integrados en empresas o profesiones aparentemente legítimas. Determinados grupos delictivos organizados adoptan estructuras que recuerdan a lugares de trabajo legítimos, aprovechando los conocimientos o habilidades adquiridos al operar en esferas ambiguas o no reguladas, al margen de las normas empresariales o comerciales convencionales. Esto puede implicar el establecimiento de una plantilla asalariada y la aplicación de una división del trabajo perfectamente definida, imitando de hecho los marcos organizativos que se encuentran en las empresas legales. No existe un grupo delictivo organizado típico que se dedique al fraude. Puede ser cometido por grupos diversos, como redes de ciberdelincuentes que comercian anónimamente con tecnologías, datos y otros servicios delictivos; grupos delictivos organizados que se agrupan en torno a una localidad o a redes sociales; grupos delictivos organizados estructurados para imitar a una plantilla legítima (por ejemplo, centros de llamadas); y delincuentes de guante blanco que cometen fraudes desde dentro de organizaciones u ocupaciones por lo demás legítimas. En lugar de jerarquías, los grupos delictivos organizados suelen presentar una colaboración fluida entre sus miembros.

---

[1] Véanse las resoluciones del Consejo Económico y Social 2004/26, 2007/20, 2009/22, 2011/35 y 2013/39, relativas a la cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad.

[2] Agencia de la Unión Europea para la Cooperación Policial (Europol), *Internet Organized Crime Threat Assessment (IOCTA) 2023* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2023); y Organización Internacional de Policía Criminal (INTERPOL), “Informe resumido sobre las tendencias de la delincuencia a escala mundial - INTERPOL 2022” (octubre de 2022).

[3] INTERPOL, “Evaluación de INTERPOL sobre estafas: un peligro mundial incrementado por la tecnología”, 11 de marzo de 2024.

7. Sin embargo, no es tanto la forma en que se organizan los delincuentes, sino más bien el modo en que se orquestan las actividades fraudulentas, lo que podría dar una idea más clara del fraude organizado. Históricamente, al fraude no se le ha concedido el mismo grado de prioridad que a otros tipos de delincuencia organizada, y a menudo el fraude organizado se ha percibido como una actividad delictiva complementaria de los grupos delictivos organizados implicados en otros delitos más graves (por ejemplo, el tráfico de drogas)[4]. En la Convención contra la Delincuencia Organizada, el delito grave se define como un delito punible con una pena máxima de al menos cuatro años de prisión. En la práctica, sin embargo, muchos Estados no tipifican el fraude como delito grave. En consecuencia, queda fuera del ámbito de aplicación de la Convención contra la Delincuencia Organizada. Además, incluso en los casos en que el fraude es punible como delito grave, la condena no refleja necesariamente esa gravedad.

II. Categorías de fraude organizado

8. El fraude es un delito que abarca acciones y comportamientos muy diversos que se llevan a cabo en una amplia gama de entornos y contra víctimas diversas. En la investigación académica, el fraude se ha definido en sentido amplio como "la obtención de algo de valor o la elusión de una obligación mediante engaño"[5]. Por lo tanto, a diferencia de otras formas de delitos graves contra el patrimonio, el fraude se perpetra mediante el engaño en lugar de la fuerza o la coacción. Además, la víctima y el autor del delito rara vez tienen que estar en el mismo lugar al mismo tiempo, y muchos fraudes cruzan fronteras nacionales e internacionales. El fraude figura en la legislación penal de muchos países, aunque se describe de diferentes maneras y con distintos grados de concreción[6]. Algunas leyes ofrecen una descripción generalizada de las conductas que constituyen fraude, mientras que otras hacen referencia a determinadas actividades, productos o servicios que destacan en las tramas fraudulentas, como la suplantación de una autoridad o la manipulación o el uso no autorizado de datos. Algunos Estados han establecido legislación diferenciada para combatir distintas facetas del delito de fraude, por ejemplo, el fraude informático, el fraude crediticio, el fraude en subastas o el fraude contra empresas. Sin embargo, hay algunos elementos básicos del fraude que figuran en la mayoría de las definiciones jurídicas: el uso del engaño para obtener una ventaja o beneficio injustos, causando un perjuicio a otra persona u organización. Por engaño suele entenderse la falta de honradez, la representación engañosa, la superchería, el artificio, las maniobras fraudulentas, el abuso de confianza o la ocultación u omisión de información. El perjuicio para otro está en muchos casos implícito en el beneficio para los autores del delito, pero en algunas definiciones se resalta el perjuicio para otro utilizando términos como afectar o perjudicar los intereses financieros de otros, una pérdida ilícita o ser defraudado. El perjuicio puede ser para un particular, una empresa o un Estado.

9. Los delitos de fraude son muy diversos en cuanto a los métodos empleados, las entidades contra las que van dirigidos y el impacto en las víctimas y en los sistemas en general. En consecuencia, se han elaborado multitud de tipologías para interpretar la naturaleza del fraude. Aunque existen otras tipologías de fraude reconocidas en los planos nacional e internacional, el presente documento de antecedentes se centra en el fraude dirigido contra personas o instituciones públicas o privadas con el fin de obtener un beneficio económico u otro beneficio material. Para ilustrarlo, se

[4] Michael Levi, "Organized fraud" en The Oxford Handbook of Organized Crime, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014).

[5] Grace M. Duffield y Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, núm. 199 (Canberra, Instituto Australiano de Criminología, 2001).

[6] Se examinaron las definiciones jurídicas de 26 países de siete regiones diferentes: Europa y América del Norte; América Latina y el Caribe; Norte de África y Asia Occidental; África Subsahariana; Asia Centromeridional; Asia Oriental y Sudoriental; y Australia y Nueva Zelandia.

definieron las siguientes categorías clave, que se explicarán con más detalle en las secciones siguientes del documento de antecedentes: a) fraude en productos y servicios de consumo; b) fraude en la inversión de los consumidores; c) fraude relacionado con el empleo; d) fraude basado en las relaciones y la confianza; e) fraude consistente en la suplantación de funcionarios u oficiales; f) falsificación de identidad; y g) fraude contra empresas u organizaciones.

10. Dentro de las categorías clave, se resaltan las formas principales de engaño relacionadas con el beneficio o el resultado que espera la víctima de la transacción fraudulenta. Aunque estas categorías no son patrimonio exclusivo de los grupos delictivos organizados, la capacidad de delinquir y causar daños aumenta considerablemente con su implicación. Cada categoría representa una técnica diferente para manipular a las víctimas, pero todas las categorías pueden ser transnacionales e implicar a coautores que colaboran en un grupo delictivo organizado. Algunas se cometen en grandes cantidades y tienen un gran efecto global, mientras que en otras, el daño lo padecen intensamente grupos más reducidos de víctimas.

A. Fraude en productos y servicios de consumo

11. Los fraudes en productos y servicios de consumo representan uno de los tipos de fraude más frecuentes, dado que hay un elevado número de ciudadanos que denuncian haber sido estafados, haber recibido comunicaciones de venta de productos o servicios fraudulentos o haberse visto expuestos a ellas. Este tipo de fraude consiste en la venta de productos o servicios inexistentes o muy distintos de los anunciados. Por lo general, los defraudadores comercializan productos de gran demanda u ofrecen productos y servicios a un coste inferior al disponible en el mercado legítimo. Algunos defraudadores dirigen sus anuncios a los grupos considerados más susceptibles de ser víctimas de una estafa concreta. Los fraudes pueden implicar vendedores y artículos totalmente ficticios, pero también empresas que dan una imagen falsa de los bienes o servicios que suministran. Puede haber dificultades para confirmar un fraude cuando el producto o servicio se recibe pero se considera que no corresponde a lo que se había hecho creer. A veces, los defraudadores se aprovechan de la falta de conocimientos financieros de la víctima para venderle servicios financieros como préstamos, planes de seguros o productos de pensiones. Suelen referirse a productos cuyo valor reside en el futuro, y a las víctimas se les ofrece una previsión excesivamente optimista de los resultados futuros o no se les explican adecuadamente los riesgos. Los defraudadores también pueden no informar a la víctima de los gastos, las comisiones o los requisitos legales, lo que puede acarrear más pérdidas y penalizaciones[7].

12. Entre los productos y servicios que suelen aparecer en los fraudes en productos y servicios de consumo figuran las piedras preciosas, los animales domésticos, las entradas para eventos, los productos médicos, las loterías o sorteos de premios que prometen grandes recompensas, o productos y servicios financieros como los seguros. Sin embargo, existe una variedad casi infinita de productos y servicios que pueden utilizarse en las maquinaciones fraudulentas, ya que los defraudadores tratan de adaptarse continuamente y sacar partido de los nuevos mercados y demandas de los consumidores.

13. Para comercializar los productos y servicios se utilizan diversos medios, especialmente Internet. Cabe citar los sitios web falsos, los sitios legítimos de compras y subastas, el correo electrónico no deseado, el correo postal o las llamadas “salas de calderas” que realizan grandes volúmenes de llamadas de comercialización y venta. Algunos delincuentes se aprovechan del dinámico mercado de listas de clientes potenciales recopiladas por medios legítimos o ilegítimos (como una violación de datos o una campaña de suplantación de identidad en línea) o incluso de directorios de personas que han sido víctimas anteriormente (las denominadas listas

[7] Véase Michael Skidmore, *Protecting People’s Pensions: Understanding and Preventing Scams* (Londres, The Police Foundation, 2020).

de “inocentones”). Las tecnologías de la información y la comunicación han aumentado enormemente la capacidad de comercializar y vender productos y servicios a escala mundial y a un coste comparativamente bajo. En algunos casos, el consumidor individual puede perder dinero, pero dependiendo de las circunstancias y los métodos empleados por los delincuentes, una plataforma de ventas o un proveedor de servicios financieros puede incurrir en la pérdida financiera. Entre las metodologías clave cabe citar:

a) Sitios web falsos creados con fines de comercialización o venta de productos y servicios. Los delincuentes pueden comercializar el sitio web utilizando canales digitales, como los medios sociales o el correo electrónico basura, o pueden manipular los motores de búsqueda de Internet para aumentar la probabilidad de que quienes buscan productos o servicios determinados aterricen en su sitio web;

b) Vendedores falsos en plataformas legítimas de venta, subasta o medios sociales que utilizan cuentas abiertas con identidades falsas o robadas. Estos vendedores explotan plataformas legítimas que dan acceso a un gran volumen de usuarios que buscan productos y servicios. Por ejemplo, un grupo delictivo organizado publicó cientos o miles de anuncios de artículos de gran valor, como automóviles, en múltiples sitios de subastas[8].

14. El fraude al consumidor en línea no tiene por qué ser sofisticado ni complejo. Para aprovechar fraudulentamente un sitio legítimo de ventas o subastas puede bastar con que una sola persona abra una cuenta en un sitio de subastas y publique un anuncio para vender un producto inexistente. Sin embargo, una parte de los delitos de fraude al consumidor son transnacionales e implican a grupos delictivos organizados. La organización rara vez queda al descubierto en el intercambio con la víctima, sino más bien al comprender la planificación y preparación que hay detrás. Entre las etapas clave cabe citar el establecimiento y la comercialización del perfil de la plataforma o sitio web, la captación de víctimas para mantener el engaño (o conseguir nuevos pagos) y el movimiento del dinero. Los delincuentes adoptan diversos métodos para recibir los pagos dejando un rastro financiero limitado. Entre los métodos cabe citar convencer a un proveedor de servicios de pago de que su empresa es legítima, desviar a los clientes a sitios de pago falsos, pedir a las víctimas que paguen con tarjetas de débito prepagadas o el uso de cuentas de terceros, bien de “mulas de dinero” o bien abiertas con identidades robadas o falsas. Los grupos delictivos organizados que operan desde otras jurisdicciones suelen reclutar a coautores dentro del país en el que realizarán el fraude para facilitar el blanqueo de dinero[9].

B. Fraude en las inversiones

15. Los fraudes en las inversiones suelen consistir en la venta de divisas, acciones o bonos de empresas, y algunas estafas comercializan inversiones en bienes muebles que van desde promociones inmobiliarias o comerciales hasta vinos y licores.

16. La comisión de estos fraudes puede requerir un agudo conocimiento de los contornos de la normativa y los controles conexos que regulan los mercados, y la línea que separa la práctica legítima de la ilegítima puede ser tan permeable como difícil de percibir. En algunos casos, los delincuentes explotan los mecanismos de confianza registrándose como una entidad regulada o explotando a otros agentes legítimos con

[8] Puede consultarse más información en Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (portal SHERLOC), Base de datos de jurisprudencia, *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*. Disponible en https://sherloc.unodc.org/.

[9] Christine Conradt, “Online auction fraud and criminological theories: the Adrian Ghighina case”, vol. 6, núm. 1, *International Journal of Cyber Criminology*, (enero/junio de 2012); y Jack M. Whittaker y Mark Button, “Understanding pet scams: a case study of advance fee and non-delivery fraud using victims’ accounts”, *Journal of Criminology*, vol. 53, núm. 4 (septiembre de 2020).

estatus regulado. Al ocupar esta zona gris entre la práctica legítima y la ilegítima, crean obstáculos a las fuerzas del orden u otros reguladores que deben sortearlos y presentar pruebas suficientes y sólidas del engaño y demostrar que se ha producido un delito. De hecho, aunque poco éticos, algunos pueden emplear métodos que causan un gran perjuicio a los inversores pero que resultan no ser delictivos. Las estafas piramidales y Ponzi son un modelo común de operación de los delincuentes; la estafa inversora se basa en atraer continuamente a nuevos inversores para seguir alimentándose, en lugar de generar rendimientos a partir de productos o inversiones genuinos, que pueden incluso no existir.

17. El fraude en las inversiones parece ir en aumento, en parte debido al incremento de los fraudes relacionados con inversiones en criptomonedas. Este nuevo medio para el fraude en las inversiones aprovecha la rapidez y agilidad que ofrecen los espacios digitales, y permite a los delincuentes realizar una comercialización masiva con rapidez y a un coste relativamente bajo[10]. En los mercados financieros nuevos, como el de las criptomonedas, las dificultades para regularlos crean mayores lagunas que explotar. Los métodos que se emplean en los fraudes en las inversiones con criptomonedas varían tanto en complejidad técnica como en novedad, y se adoptan algunas técnicas procedentes de otros métodos, como la manipulación del mercado y la captación financiera, que incluyen la creación y comercialización de plataformas fraudulentas de inversión en criptomoneda y las denominadas "estafas de salida" o "tirones de alfombra" que implican inflar artificialmente el valor de los vehículos de la estafa, que pierden completamente su valor una vez que los delincuentes retiran todo el dinero invertido.

18. El éxito de los fraudes en las inversiones depende de una comunicación eficaz, utilizando diversas técnicas para persuadir a los posibles inversores, como campañas de comercialización selectivas o masivas; técnicas de venta agresivas; y la producción de recursos para establecer y mantener la credibilidad y la confianza, como gestión de marcas, sitios web y otros materiales de comercialización. Los delincuentes pueden utilizar canales de comunicación específicos, o una combinación de ellos, que se despliegan en distintas fases del delito. Por ejemplo, el contacto inicial con una víctima puede producirse a través de un sitio web de suplantación de identidad, al que sigue una llamada telefónica de ventas y, posteriormente, un contacto continuado a través de un sitio web fraudulento. Los defraudadores pueden utilizar los métodos siguientes para relacionarse con las víctimas:

a) Venta telefónica: el uso de centros de llamadas o "salas de calderas" para comercializaciones y ventas agresivas, a menudo en forma de llamadas no solicitadas a personas que se escogen utilizando listas de clientes potenciales recopiladas o compradas a otros agentes legítimos o ilegítimos que recopilan y venden esta información personal sobre los consumidores. En algunos casos, esas listas incluyen a personas de las que se sabe que han sido víctimas con anterioridad y, por tanto, son vulnerables a planteamientos de inversión similares, un problema que es especialmente grave en el caso de las víctimas vulnerables de edad avanzada. Los centros de llamadas pueden ser gestionados directamente por los delincuentes que operan las actividades fraudulentas o contratados a especialistas capaces de prestar esos servicios de "sala de calderas". Estos centros pueden estar situados en países extranjeros para las víctimas, a veces en jurisdicciones conocidas por tener controles menos sólidos sobre estas actividades[11];

b) En línea: en algunos países se ha producido un aumento considerable de los fraudes en las inversiones en línea, en los que el contacto inicial se realiza a través de comunicaciones en línea, como medios sociales, sitios web fraudulentos y aplicaciones, que desempeñan una función decisiva en el engaño. La accesibilidad de

[10] Arianna Trozze, Toby Davies y Bennett Kleinberg, "Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering", vol. 46, *Journal of Forensic Science International: Digital Investigation* (2023).

[11] Neal Shover, Glenn. S. Coffe y Clintin R. Sanders, "Dialing for dollars: opportunities, justifications, and telemarketing fraud", *Qualitative Sociology*, vol. 27, núm. 1 (marzo de 2004).

las tecnologías digitales y los grandes conjuntos de datos sobre los consumidores aumentan enormemente la capacidad de realizar una comercialización selectiva y a gran escala. Por ejemplo, pueden utilizarse campañas de suplantación de identidad para atraer y localizar a personas interesadas en el producto o servicio que se ofrece, lo que sirve de base para orientar la comunicación posterior. Los autores suelen explotar los medios sociales y las aplicaciones de comunicación digital para comercializar sus productos, y en algunos casos utilizan imágenes de personas famosas o de la cultura popular para persuadir a las víctimas de que inviertan su dinero. Cuando estas maquinaciones fraudulentas con criptomonedas penetran en los mercados financieros convencionales, pueden causar pérdidas financieras asombrosas;

c) En persona: las inversiones a menudo implican grandes sumas de dinero que resultan muy considerables para las víctimas, y en algunos casos el contacto cara a cara sigue siendo importante para lograr niveles de confianza suficientes para lograr una inversión. Algunos defraudadores escogen a las víctimas a partir de conexiones sociales o comerciales existentes para explotar una confianza que ya existe.

19. Los defraudadores en inversiones hacen todo lo posible por cultivar un barniz de legitimidad y suelen adoptar las estructuras, los procesos y el lenguaje de una organización oficial legítima, incluida una clara división del trabajo, con una jerarquía y funciones asignadas al personal. La complejidad de la operación es variable, dependiendo de su motivación para evitar sospechas o ser detectados y seguir delinquiendo [12]. Las denominadas operaciones "*rip and tear*" pueden funcionar durante breve plazo antes de desaparecer con el dinero de los inversores, mientras que otras estafas pueden operar sin ser detectadas durante muchos años.

20. Las víctimas de fraudes en las inversiones sufren las pérdidas más elevadas en comparación con otros fraudes dirigidos contra particulares [13]. A las víctimas se les inculcan expectativas de rentabilidad económica totalmente falsas o sumamente exageradas. Muchos inversores pierden todo o gran parte de su dinero. Independientemente del método concreto que se emplee, a las víctimas se les suele vender una expectativa del valor que obtendrán de su inversión en un futuro, lo que significa que pueden pasar años desde la inversión inicial antes de que se den cuenta de que han sido víctimas. Las particularidades de las distintas estafas y el engaño subyacente pueden ser muy variables, pero el resultado suele ser que los inversores pierden todo su dinero o gran parte de él. He aquí algunos ejemplos:

a) Un engaño completo, en el que el servicio o producto de inversión nunca existió;

b) La venta abusiva de acciones sin valor o sobrevaloradas para inversiones de alto riesgo que probablemente no producirán el rendimiento prometido o simplemente pueden fallar;

c) Técnicas de manipulación del mercado que inflan artificialmente el valor de las inversiones ante inversores desprevenidos.

21. La importancia de la pérdida pecuniaria para las víctimas dependerá de sus circunstancias financieras o personales. También puede depender de las metodologías empleadas por los delincuentes; por ejemplo, captar los ahorros de las pensiones de las personas puede afectar en gran medida a cada una de las víctimas [14], mientras que algunas inversiones en criptomonedas pueden ir dirigidas a recibir cantidades más pequeñas pero de un mayor número de víctimas. En el caso de las víctimas de estafas piramidales y Ponzi, es posible que quienes invierten y retiran dinero en una fase temprana no pierdan dinero. Una vez robado el dinero, la víctima puede ser

[12] Michael Levi, "Organized fraud and organizing frauds: unpacking research on networks and organization", *Criminology and Criminal Justice*, vol. 8, núm. 4 (diciembre de 2008).

[13] Véase también Departamento de Justicia de los Estados Unidos de América, "Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes", comunicado de prensa, 3 de abril de 2023.

[14] Véase Skidmore, *Protecting People's Pensions*.

revictimizada por los mismos delincuentes o por otros, en algunos casos simulando pertenecer a un organismo legítimo. Afirman ser capaces de rastrear y recuperar los fondos perdidos, pero exigen a la víctima una comisión por adelantado, un fraude conocido como fraude de recuperación.

C. Fraude relacionado con el empleo

22. El fraude relacionado con el empleo consiste en la comercialización masiva de ofertas de empleo falsas o engañosas en sitios web de ofertas de empleo. El uso de anuncios de empleo en línea ha crecido considerablemente en el sector legal, sobre todo desde la pandemia mundial, en la que quienes contratan personal ofrecen modalidades de trabajo más flexibles y oportunidades de trabajo desde el domicilio. Los defraudadores se aprovechan de la demanda de puestos deseables, sobre todo en los segmentos de la población en los que las oportunidades legítimas de este tipo son limitadas debido a una cualificación o formación insuficientes o a la falta de empleos disponibles en la economía local[15]. La investigación indica que estos defraudadores suelen dirigirse a los solicitantes de empleo menos seguros económicamente o en situaciones desesperadas.

23. Estos fraudes suelen consistir en anunciar en Internet una oportunidad de empleo que, o bien es totalmente ficticia, o bien es mucho menos rentable de lo que se anuncia. Por ejemplo, cabe citar anuncios de oportunidades de negocio, trabajo desde casa u oportunidades de modelaje. En algunos casos, los defraudadores solicitan pagos por adelantado a las víctimas antes de ocupar un puesto; las supuestas razones son múltiples, como los kits de iniciación, los viajes, la formación o las comprobaciones de calificaciones crediticias. El resultado suele ser que la víctima pierde dinero sin recibir el empleo prometido. En otras estafas, los defraudadores envían cheques falsos a las víctimas para pagarles los gastos iniciales antes de afirmar que han realizado un sobrepago y solicitar a la víctima que transfiera el dinero excesivo de vuelta al delincuente. La víctima pierde el dinero transferido y se queda con el coste del cheque una vez detectado como falso.

24. El objetivo de quienes estafan con ofertas de empleo puede ser también robar información personal de identidad, que las víctimas facilitan durante el proceso de solicitud, dejándolas vulnerables para nuevas victimizaciones. Y en algunos casos el trabajo resulta ser de naturaleza delictiva. Por ejemplo, la víctima puede verse arrastrada a facilitar el blanqueo de dinero (entre otros medios, como “mula de dinero”) o a actuar como mensajero para entregar artículos adquiridos fraudulentamente (es decir, falsificación de identidad). En los casos más graves, la víctima se convierte en objeto de trata de personas para trabajos forzosos y delincuencia forzada[16].

D. Fraude basado en las relaciones y la confianza

25. Los procesos para establecer la confianza desempeñan una función decisiva en cualquier tipo de fraude. Sin embargo, en el caso del fraude basado en las relaciones y la confianza, los delincuentes fomentan y explotan el poder de las relaciones personales con objeto de desarrollar la confianza necesaria para manipular y engañar a las víctimas, a veces en múltiples ocasiones. En estos fraudes, la víctima no espera recibir un producto o servicio, sino entablar una verdadera relación con el delincuente.

---

[15] Alexandrea J. Ravenelle, Erica Janko y Ken Cai Kowalski, “Good jobs, scam jobs: detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic”, *New Media and Society*, vol. 24, núm. 7 (julio de 2022), págs. 1.591 a 1.610; y Delali Kwasi Dake, “Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites”, *International Journal of Computer Applications*, vol. 184, núm. 51 (marzo de 2023).

[16] Puede consultarse más información sobre estas dos formas de explotación en Informe *mundial sobre la trata de personas 2002* (publicaciones de las Naciones Unidas, 2022), así como en UNODC, “Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: policy report” (Bangkok, 2023).

La complejidad de estos fraudes reside menos en la explotación de sistemas técnicos o tecnológicos y más en la dinámica de la relación entre la víctima y el autor del fraude.

26. Muchos defraudadores establecen relaciones en línea y utilizan técnicas de ingeniería social durante meses o incluso años para ganarse la confianza de la víctima. Las víctimas suelen esperar una relación romántica, pero el fraude también puede adoptar otras formas, como una amistad de confianza, o incluso el deseo de una relación con un familiar de la víctima. Varios estudios han detectado vulnerabilidades en la población de edad avanzada relacionadas con factores como la soledad, el aislamiento social y el deseo de entablar nuevas relaciones. Los delincuentes buscan y explotan esa vulnerabilidad mediante un proceso de amistad o compromiso romántico. Además, los delincuentes pueden hacerse pasar por un familiar o amigo que se encuentra en graves dificultades y necesita dinero para remediar la situación. Estos fraudes pueden ser selectivos e incorporar datos personales extraídos de publicaciones en medios sociales del amigo o familiar para hacer más creíble la comunicación con la víctima. Esto se comunica habitualmente por mensaje de texto. Hay ejemplos de inteligencia artificial utilizada para clonar la voz de un familiar o amigo en una llamada telefónica.

27. Un elemento central de esta categoría de fraude es el fraude romántico, en el que los delincuentes establecen relaciones románticas en línea con el propósito de engañar y extorsionar a las víctimas. Las pérdidas económicas que sufren las personas en cuestión pueden ser importantes. Se trata de un problema que afecta a víctimas de muchas regiones diferentes del mundo y que aprovecha el crecimiento de las redes sociales en línea y, más concretamente, una tendencia social más amplia a encontrar relaciones románticas en línea. La aproximación inicial a las víctimas suele producirse a través de los medios sociales o los sitios web y aplicaciones de citas por parte de un delincuente que utiliza una identidad falsa junto con el historial correspondiente en su perfil. Un único delincuente puede ir cambiando entre diversas identidades para captar y atraer a una posible víctima. Una vez establecida la relación, el delincuente puede obtener un beneficio económico solicitando inicialmente una pequeña suma de dinero antes de pedir cantidades mayores a la víctima, a menudo apoyándose en una situación de crisis que sirve para aplicar presión y urgencia a la víctima (por ejemplo, una emergencia de salud o la necesidad urgente de viajar). Si se intercambiaron imágenes sexuales, también se puede extorsionar a la víctima.

28. Una encarnación más reciente de este método ha consistido en mezclar el fraude romántico con el fraude en inversiones en criptomonedas. El fraude mediante un cebo romántico o la denominada “matanza de cerdos” (“*pig butchering*”) —expresión cuyo uso no se recomienda, por respeto a las víctimas de estos delitos— implica que un delincuente fomenta una relación personal con una víctima en línea. En lugar de inventar una situación de crisis, explota la relación íntima y la confianza para atraerla a un plan de inversión fraudulento. Para los delincuentes, esto puede incorporar etapas adicionales de planificación y preparación, incluida la creación de un sitio web o una aplicación fraudulentos a los que pueda acceder la víctima, e incluso la prestación de un “servicio de atención al cliente” para los inversores[17]. La integración de las inversiones en criptomonedas en el engaño tiene una serie de consecuencias: amplía el grupo de posibles víctimas a grupos de edad más jóvenes; introduce a las víctimas en un mercado desconocido, volátil y de alto riesgo, por lo que es menos probable que reconozcan que son víctimas; e introduce más dificultades para los investigadores penales a la hora de rastrear los fondos hasta llegar a los delincuentes.

29. Gran parte de la investigación sobre el fraude romántico se ha centrado en las víctimas y sus experiencias, no en los delincuentes, que son menos visibles. Se considera que suelen ser delitos transnacionales perpetrados por grupos delictivos

[17] Cassandra Cross, “Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud”, *Current Issues in Criminal Justice* (2023); y Fangzhou Wang y Xiaoli Zhou, “Persuasive schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan (杀猪盘) in China”, *Victims and Offenders*, vol. 18, núm. 5 (2023).

organizados, con cierta concentración en determinadas regiones. En el contexto del fraude de la "matanza de cerdos", algunos grupos delictivos organizados han adoptado estructuras más elaboradas de tipo empresarial en las que existe una división clara del trabajo (por ejemplo, contacto con las víctimas, tecnología de la información y blanqueo de dinero) y la captación de una mano de obra de personas necesitadas de dinero y en riesgo de explotación, incluida la trata de personas[18].

30. Independientemente de las características de las víctimas, el impacto de un fraude basado en las relaciones y la confianza puede ser considerable. Si bien las víctimas experimentan pérdidas económicas, también sufren por la ruptura de la confianza y la pérdida de una relación personal importante. Además, padecen importantes daños psicológicos y emocionales. Algunas pueden incluso negarse a aceptar que son o han sido víctimas de un fraude.

E. Fraude consistente en la suplantación de funcionarios u oficiales

31. El fraude consistente en la suplantación de funcionarios u oficiales, o fraude por suplantación, consiste en manipular las comunicaciones para que parezcan proceder de un funcionario público o de un oficial de otro tipo, como la policía, una autoridad fiscal, un banco o un departamento de la administración pública. Estos fraudes emplean una serie de pretextos y situaciones como la suplantación de una autoridad fiscal u otro departamento de la administración pública que reclaman una deuda impagada; un oficial de un banco que afirma que el dinero de una cuenta bancaria está amenazado por delincuentes; o la policía alegando que ha detectado un delito cometido por la víctima.

32. Un rasgo distintivo esencial del fraude por suplantación de identidad es el uso de técnicas de persuasión que apelan menos a los deseos y necesidades de las víctimas (como en los fraudes a los consumidores) y, en su lugar, evocan miedo, temor, ansiedad y preocupación. Inducir un estado emocional exacerbado sirve para impedir la toma de decisiones y hace que las víctimas sean más susceptibles a la manipulación. Esos mensajes amenazan con un resultado negativo, incluido algún tipo de respuesta legal, si la víctima no envía el pago o transfiere los fondos.

33. Estos fraudes suelen implicar comunicaciones masivas, como el correo electrónico basura; las comunicaciones a través de los medios sociales; los mensajes de texto; o las llamadas telefónicas automatizadas, o las denominadas "llamadas robotizadas", en las que las llamadas telefónicas se automatizan utilizando un mensaje grabado. Estas tecnologías facilitan el contacto casi simultáneo con miles de víctimas a la vez, lo que les da un alcance inmenso.

F. Falsificación de identidad

34. La falsificación de identidad[19] implica el uso de información de identidad robada o falsa para obtener acceso directo a bienes, servicios o dinero de las víctimas; por ejemplo, el uso de información robada para hacer compras o acceder a cuentas financieras. Puede perpetrarse sin que medie comunicación o acción directa alguna por parte de la persona cuya identidad está siendo usurpada, ya que el objetivo suele ser el proveedor de los bienes, servicios o dinero. De este modo, el daño se reparte entre los diferentes actores que lo sufren, a saber, la víctima cuya identidad es objeto de abuso, el proveedor de servicios financieros u otra empresa de la que se sustrae el dinero y, en algunos casos, el proveedor de los bienes o servicios adquiridos con los fondos robados.

35. Existen diferentes formas de información de identidad que pueden adquirirse, y cada una de ellas puede explotarse de distintas maneras. Cabe citar la información personal, que comprende las identidades digitales de la persona en diferentes entornos

[18] UNODC, "Casinos, cyber fraud, and trafficking in persons".

[19] Véase también UNODC, *Manual sobre los delitos relacionados con la identidad* (Viena, 2011).

en línea, como el nombre o la fecha de nacimiento; datos de cuentas financieras, como números de tarjetas de crédito; información sobre cuentas en línea, como nombres de usuario y contraseñas; y datos biométricos, como una huella digital robada de un dispositivo electrónico.

36. Los delincuentes pueden acceder a esta información mediante la intromisión en el sistema; las estafas de ingeniería social como campañas de suplantación de identidad (*phishing)* o de mensajes fraudulentos (*smishing)*; o accediendo a mercados delictivos en línea que venden los datos. Los datos pueden utilizarse para adquirir bienes y servicios, presentar solicitudes de préstamos y otro tipo de financiación o acceder y transferir dinero de las cuentas de las víctimas. Cabe citar la siguiente información adicional sobre los medios utilizados:

a) Intromisión en el sistema: algunos defraudadores se dedican a obtener información personal mediante técnicas ilícitas de piratería informática, despliegue de programas maliciosos o suplantación de identidad;

b) Mercados delictivos en línea: existe una dinámica economía informal implicada en la compraventa de información de identidad, que puede ser explotada por los defraudadores de identidad. La oportunidad de adquirir información de esta manera elimina algunos de los obstáculos técnicos para los defraudadores, que de otro modo no dispondrían de estas capacidades para robar información personal;

c) Ingeniería social: a menudo se consigue mediante un anuncio u otra comunicación no solicitada enviados por correo electrónico u otra comunicación en línea, mensaje de texto o llamada telefónica no solicitada, mediante los cuales se engaña a las víctimas para que faciliten información personal. El grado de sofisticación es variable, pero los métodos más complejos, como la suplantación de sitios web legítimos, pueden llevar a que la seguridad quede más comprometida, al proporcionar a los delincuentes acceso directo a cuentas en línea.

37. Los delincuentes emplean diversas técnicas para cometer falsificaciones de identidad. Algunos de los métodos clave son la apropiación de cuentas, el fraude sin presencia física de tarjeta y el fraude de solicitudes, que se definen de la siguiente manera:

a) Apropiación de cuentas: en estos fraudes, los delincuentes obtienen credenciales legítimas para acceder a cuentas de usuario. Puede tratarse de cuentas bancarias, pero también de otros tipos de cuentas financieras (por ejemplo, proveedores de moneda virtual), sitios de venta al por menor o cualquier proveedor de bienes y servicios. La cuenta puede aprovecharse para fines diversos, como la transferencia directa de fondos a cuentas controladas por los delincuentes o la compra fraudulenta de bienes o servicios utilizándola. En algunos casos, adquirir información para acceder a la cuenta de una víctima es el primero de una serie de pasos necesarios para acceder al dinero, bienes o servicios a través de intromisiones posteriores en el sistema. Esto puede implicar superar medidas de seguridad como la autentificación de dos factores. En consecuencia, los delincuentes recurren a técnicas adicionales como el cambio de SIM y métodos de pago alternativos;

b) Fraude sin presencia física de tarjeta: compras no autorizadas realizadas a distancia a un vendedor, ya sea por Internet o por teléfono. La adquisición de las credenciales financieras de una víctima basta para engañar tanto al proveedor de servicios financieros como al vendedor comercial, sin necesidad de una interacción directa con la víctima ni de acceso a la tarjeta de pago física. Hay una serie de pasos clave que suelen necesitar los falsificadores de identidad para explotar las credenciales financieras de una víctima:

i) Adquirir conocimientos, recursos y credenciales financieras en los mercados delictivos en línea;

ii) Disfrazar los pedidos para evitar que se activen los algoritmos de detección de fraudes en un sitio comercial;

iii) Recibir los pedidos en una dirección que no permita localizar a los delincuentes;

iv) Revender los artículos como vendedor individual o venderlos al por mayor haciéndose pasar por un comerciante legítimo en los cibermercados establecidos;

c) Fraude de solicitudes: estos fraudes se aprovechan de la amplia disponibilidad de información personal y la utilizan para solicitar créditos en nombre de la víctima. Suele hacerse con el objetivo de obtener un préstamo de un proveedor de servicios financieros. Los delincuentes deben acceder a un conjunto de datos personales (por ejemplo, nombre, dirección o fecha de nacimiento) para poder suplantar de forma creíble a la persona. Una tendencia emergente es el uso de la tecnología para crear identidades sintéticas combinando elementos de identificación reales y falsos. Una vez establecidas, estas identidades pueden cultivarse con el tiempo para que sean más solventes antes de terminar presentando solicitudes de productos financieros de alto valor.

38. Es importante señalar que la comisión de falsificaciones de identidad no está supeditada a la implicación de la delincuencia organizada y los grupos delictivos organizados. No obstante, la capacidad para perpetrar falsificaciones de identidad a gran escala y lograr elevados beneficios se ve enormemente aumentada por las habilidades y los recursos de que dispone la delincuencia organizada. Lo que vuelve especialmente grave esta amenaza es la proliferación de posibles víctimas en línea disponibles en las economías digitales en expansión. La manipulación y el abuso de la identidad pueden servir para diversas funciones en la comisión de delitos organizados, por ejemplo maniobrar para impedir que se rastree la actividad delictiva hasta los autores[20].

G. Fraude contra empresas u organizaciones

39. El fraude contra empresas u organizaciones suele implicar el abuso de sistemas internos o de una relación comercial para defraudar a la víctima. Estos fraudes pueden ser perpetrados por alguien interno o externo a la organización. Algunos son perpetrados por empresas y actores por lo demás legítimos o que utilizan productos legítimos, en lugar de tratarse de maquinaciones concebidas desde el principio para perpetrar un fraude, a veces en respuesta a presiones internas o a prácticas o a una cultura de trabajo dudosas.

40. Algunos ejemplos de fraude contra empresas u organizaciones son los siguientes:

a) El fraude que se comete comprometiendo el correo electrónico empresarial es un fraude cibernético que se perpetra en grandes volúmenes. Empresas y organizaciones de todos los tamaños y de diversos sectores son víctimas de este tipo de fraude, habitualmente cometido por delincuentes externos. Los delincuentes se infiltran en los sistemas y utilizan técnicas de ingeniería social para persuadir al personal de que realice transferencias no autorizadas de fondos a cuentas bajo el control de los delincuentes. Las pérdidas para las víctimas pueden ser muy elevadas. Un primer paso consiste en infiltrarse en los sistemas de comunicación de una organización para hacer más fácil persuadir a los destinatarios de que son legítimos. Entre los principales métodos cabe citar la piratería informática de las cuentas de correo electrónico de los miembros del personal; el envío de correos electrónicos con suplantación de identidad para obtener datos de las cuentas de los miembros del personal; o la explotación de proveedores de comunicaciones para suplantar nombres de dominio que resulten familiares a la organización contra la que va dirigido el fraude[21].Los delincuentes adoptan diversas estratagemas, entre las que se incluyen la

[20] Simon Baechler, “Document fraud: will your identity be secure in the twenty-first century?”, *European Journal on Criminal Policy and Research*, vol. 26, núm. 3 (junio de 2020).

[21] Norah Saud Al-Musib y otros, “Business email compromise (BEC) attacks”, Materials Today:

explotación de una relación existente entre dos empresas mediante la emisión de una factura falsa; el envío de un correo electrónico supuestamente procedente de un miembro del personal de categoría superior en el que se presenta una solicitud urgente de fondos; o hacerse pasar por un abogado que solicita una transferencia electrónica para responder a un asunto delicado[22]. La comunicación puede producirse durante un periodo de tiempo y los delincuentes pueden invertir tiempo en comprender la organización y sus sistemas y victimizarlos en múltiples ocasiones;

b) Los fraudes relacionados con los estados financieros incluyen una multitud de métodos en los que profesionales por lo demás legítimos de un mercado financiero engañan y distorsionan las percepciones de otros, como inversores, reguladores y otros agentes del mercado, sobre la salud financiera y las perspectivas futuras de una empresa o fondo. Tipos similares de fraude contable también pueden encubrir la apropiación indebida, la malversación o el desfalco de fondos. Estos fraudes pueden perpetrarse en respuesta a presiones para cumplir las expectativas de rendimiento. Cabe citar, por ejemplo, a ejecutivos de empresas, operadores financieros deshonestos o gestores de fondos de inversión libre que informan sobre resultados financieros. En algunos casos, las consecuencias de estos fraudes se dejan sentir fuera de la empresa, por ejemplo en empresas externas, sectores o incluso la economía en general[23];

c) Los fraudes con sociedades a corto o largo plazo pueden ser perpetrados por empresas comercializadoras existentes o por empresas que pueden haber sido adquiridas o creadas con fines fraudulentos. Las empresas establecen un historial de crédito, confianza o credibilidad, que se utiliza con objeto de engañar a un comprador, vendedor o acreedor para que suministre bienes o financiación. Las sociedades lo hacen a sabiendas de que no pueden pagar o no tienen intención de hacerlo.

III. Cuestiones que se someten a consideración

41. El Grupo de Trabajo tal vez desee centrar sus deliberaciones en las cuestiones siguientes:

a) La naturaleza del fraude organizado en diversas jurisdicciones;

b) La utilización de la Convención contra la Delincuencia Organizada para prevenir y combatir el fraude organizado, así como la tipificación del fraude como delito grave, conforme a la definición del artículo 2 de la Convención;

c) Las oportunidades para una cooperación internacional eficaz, también con el sector privado;

d) El intercambio de información sobre la prevención del fraude organizado, la protección de las víctimas y testigos de fraudes, así como de los denunciantes de irregularidades, y la persecución de los grupos delictivos organizados implicados en el fraude organizado, así como el fomento de asociaciones con esos fines;

e) La determinación de las necesidades de asistencia técnica pertinentes en relación con la aplicación de la Convención contra la Delincuencia Organizada para prevenir y combatir el fraude organizado.

Proceedings (vol. 81, Parte 2 (2023)); y Geoffrey Simpson, Tyler Moore y Richard Clayton, “Ten years of attacks on companies using visual impersonation of domain names”, documento de investigación presentado en el Simposio sobre Investigaciones de Delitos Electrónicos (eCrime), organizado por el Grupo de trabajo de lucha contra las estafas por Internet y celebrado en Boston (Estados Unidos de América) del 16 al 19 de noviembre de 2020.

[22] Alessandro E. Agazzi, “Business Email Compromise (BEC) and cyberpsychology”. Puede consultarse en https://arxiv.org/; y Al-Musib y otros, “Business email compromise (BEC) attacks”.

[23] Reino Unido de Gran Bretaña e Irlanda del Norte, Fiscalía de Delitos Económicos Graves, “Senior bankers sentenced to 9 years for rigging EURIBOR rate”, 1 de abril de 2019.

IV. Seguimiento y posibles recomendaciones

42. El Grupo de Trabajo tal vez desee formular las siguientes recomendaciones:

a) Alentar a los Estados que aún no lo hayan hecho a considerar la posibilidad de tipificar el fraude como como delito grave, tal como se define en el artículo 2, apartado b), de la Convención contra la Delincuencia Organizada, a fin de que, en los casos de delitos de carácter transnacional en los que esté involucrado un grupo delictivo organizado, pueda prestarse una cooperación internacional eficaz en el marco de la Convención;

b) Instar a los Estados partes a que utilicen los instrumentos que ofrece la Convención contra la Delincuencia Organizada para elaborar o modificar la legislación nacional, según sea necesario y apropiado, para prevenir y combatir el fraude, en especial el fraude cometido por grupos delictivos organizados;

c) Alentar a los Estados partes a que analicen, en consulta con otras partes interesadas pertinentes, cuando proceda, las tendencias de las actividades de los grupos delictivos organizados en relación con el fraude organizado y a que comuniquen esa información y esos datos a la Oficina de las Naciones Unidas contra la Droga y el Delito;

d) Solicitar a la Oficina de las Naciones Unidas contra la Droga y el Delito que, a reserva de la disponibilidad de recursos extrapresupuestarios, recopile, analice y difunda información relativa al fraude organizado;

e) Instar a los Estados partes a que se presten mutuamente la más amplia cooperación internacional, incluida la asistencia judicial recíproca, en investigaciones, enjuiciamientos y actuaciones judiciales relacionados con el fraude organizado y los delitos conexos contemplados en la Convención contra la Delincuencia Organizada y sus Protocolos;

f) Alentar a los Estados partes a que refuercen su cooperación con las partes interesadas pertinentes, como el sector privado, las organizaciones de la sociedad civil, los medios de comunicación, el mundo académico y la comunidad científica, en la prevención y la lucha contra el fraude organizado, en particular mediante campañas de educación y sensibilización;

g) Solicitar a la Oficina de las Naciones Unidas contra la Droga y el Delito que, con sujeción a la disponibilidad de recursos extrapresupuestarios, siga preparando herramientas de asistencia técnica y prestando a los Estados partes que la soliciten asistencia técnica, incluso para el fomento de la capacidad, a fin de apoyar sus iniciativas para aplicar eficazmente la Convención contra la Delincuencia Organizada para prevenir y combatir el fraude organizado;

h) Pedir a los Estados partes que aún no lo hayan hecho que actualicen sus registros legislativos sobre la tipificación del fraude organizado en el portal de gestión de conocimientos Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC).