Nations Unies CTOC/COP/WG.2/2024/3

Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée

Distr. générale
25 mars 2024
Français
Original : anglais

Groupe de travail d'experts gouvernementaux sur l'assistance technique
Vienne, 3 et 4 juin 2024
Point 3 de l'ordre du jour provisoire*
Fraude organisée

Fraude organisée

Document d'information établi par le Secrétariat

I. Introduction

1. Le présent document d'information a été établi par le Secrétariat pour faciliter les discussions que le Groupe de travail d'experts gouvernementaux sur l'assistance technique doit tenir à sa quinzième réunion au titre du point 3 de l'ordre du jour provisoire. Il donne un bref aperçu, non exhaustif, des différentes catégories de fraude organisée qui sont utilisées pour cibler des individus ou des institutions dans le but d'obtenir un avantage financier ou un autre avantage matériel et vise à promouvoir des réponses plus efficaces à la fraude organisée dans le cadre de la Convention des Nations Unies contre la criminalité transnationale organisée.

2. La fraude a considérablement évolué au fil des ans, les criminels s'adaptant aux progrès technologiques et aux évolutions de la société. De plus en plus élaborée, elle recourt à la manipulation psychologique et à la technologie, à l'apprentissage automatique, à l'intelligence artificielle et à d'autres technologies pour automatiser les délits. De par sa fréquence élevée et sa gravité, la fraude présente un risque considérable pour les populations, les économies et la prospérité dans le monde, et compromet la confiance qu'a le public en l'état de droit. Cependant, on se heurte, lorsque l'on cherche à comprendre précisément ce phénomène, à plusieurs problèmes. Souvent, les victimes ne signalent pas les fraudes en raison d'un sentiment de honte, de culpabilité ou d'embarras, ainsi que du fait qu'elles ne reconnaissent pas qu'un délit a été commis. En outre, une part importante de la fraude vise les entreprises, dont beaucoup choisissent de ne pas signaler ces délits pour ne pas nuire à leur réputation. L'anonymat et l'éloignement associés à la perpétration de fraudes dissimulent encore davantage l'identité des délinquants aux yeux des victimes et des autorités, ce qui entrave les efforts faits pour évaluer les schémas sous-jacents et les risques associés. En outre, du fait de la nature dynamique de la fraude, qui s'adapte constamment à l'évolution des systèmes juridiques, sociaux, commerciaux et technologiques, il se peut que des méthodes de commission de délits nouvelles et innovantes passent inaperçues dans les données officielles statiques.

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

V.24-05658 (F) 100524 130524

3. La communauté internationale a pris conscience de l'ampleur inquiétante de la fraude et de la nécessité d'agir de concert pour la prévenir et la combattre[1]. Dans sa résolution 78/229, l'Assemblée générale a réaffirmé le mandat qui a été confié à l'Office des Nations Unies contre la drogue et le crime (ONUDC) d'aider, à leur demande, les États Membres par une coopération et une assistance techniques concernant toutes les formes de criminalité organisée, y compris la fraude. Cela correspond à l'objet de la Convention contre la criminalité organisée, qui vise à promouvoir la coopération pour prévenir et combattre plus efficacement la criminalité transnationale organisée, comme l'indique son article premier. Consciente de l'évolution de la nature de la fraude et de l'utilisation croissante qui est faite de la technologie pour en élargir la portée, l'Assemblée générale, dans sa résolution 74/177, a demandé aux États Membres d'envisager les mesures à prendre, ainsi que les conclusions et recommandations à formuler, pour mettre en place un cyberenvironnement sûr et résilient, en accordant une attention particulière aux délits d'usurpation d'identité.

4. Il est largement reconnu que la fraude peut relever de la criminalité organisée et être une infraction grave[2]. L'évolution de la technologie et l'expansion rapide de la portée et de l'ampleur de la criminalité organisée ont conduit à la création d'une série de nouveaux moyens de frauder les particuliers, les entreprises et même les gouvernements à une échelle massive et mondiale. Cela a permis aux groupes criminels organisés de cibler plus efficacement les victimes dans le monde entier[3].

5. Dans le domaine de la criminalité organisée, la fraude présente des caractéristiques distinctes. Tout d'abord, il s'agit avant tout de vol d'argent plutôt que de production ou de distribution de biens illégaux, ce qui la distingue des autres activités criminelles. Deuxièmement, de nombreuses activités frauduleuses sont menées à distance, facilitées par la technologie qui permet une communication anonyme et le transfert de fonds volés sans interaction physique entre l'auteur et la victime. Troisièmement, la fraude repose souvent sur le fait que les victimes donnent volontairement accès à leurs fonds, le succès dépendant de tactiques trompeuses qui brouillent la frontière entre les entités légitimes et illégitimes. Ces éléments façonnent les méthodes employées par les fraudeurs, déterminent les capacités nécessaires et influencent la structure des groupes criminels organisés.

6. Certains de ces fraudeurs sont intégrés dans des entreprises ou des professions apparemment légitimes. Utilisant les connaissances ou les compétences acquises en opérant dans des domaines flous ou non réglementés, en dehors des normes commerciales traditionnelles, certains groupes criminels organisés adoptent des structures qui rappellent les lieux de travail légitimes. Cela peut impliquer la mise en place d'une main-d'œuvre salariée et l'instauration d'une division du travail bien définie imitant les cadres organisationnels que l'on trouve dans les entreprises légales. Il n'existe pas, pour ce qui est de pratiquer la fraude, de groupe criminel organisé typique. La fraude peut être commise par divers groupes, y compris des réseaux cybercriminels qui échangent anonymement des technologies, des données et d'autres services criminels ; des groupes criminels organisés qui se regroupent autour d'une localité ou de réseaux sociaux ; des groupes criminels organisés structurés de manière à imiter une main-d'œuvre légitime (par exemple, des centres d'appel) ; et des criminels en col blanc qui commettent des fraudes au sein d'organisations ou de

[1] Voir les résolutions 2004/26, 2007/20, 2009/22, 2011/35 et 2013/39 du Conseil économique et social sur la coopération internationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l'identité.

[2] Agence de l'Union européenne pour la coopération des services répressifs (Europol), *Internet Organized Crime Threat Assessment (IOCTA) 2023* (Luxembourg, Office des publications de l'Union européenne, 2023) ; et Organisation internationale de police criminelle (INTERPOL), « 2022 INTERPOL global crime trend summary report » (octobre 2022).

[3] INTERPOL, « INTERPOL financial fraud assessment: a global threat boosted by technology », 11 mars 2024.

professions par ailleurs légitimes. Au lieu de hiérarchies, les groupes criminels organisés se caractérisent souvent par une collaboration fluide entre leurs membres.

7. Toutefois, ce n'est pas tant la manière dont les délinquants sont organisés que la manière dont les activités frauduleuses sont orchestrées qui pourrait permettre de mieux comprendre la fraude organisée. Par le passé, la fraude n'a pas bénéficié des mêmes niveaux de priorité que les autres types de criminalité organisée, la fraude organisée étant souvent perçue comme une activité criminelle supplémentaire de groupes criminels organisés auteurs d'autres infractions plus graves (par exemple, le trafic de drogue)[4]. Dans la Convention contre la criminalité organisée, l'infraction grave est définie comme un délit passible d'une peine d'au moins quatre ans d'emprisonnement. Dans la pratique, cependant, de nombreux États ne considèrent pas la fraude comme une infraction grave. Elle ne relève donc pas du champ d'application de la Convention contre la criminalité organisée. En outre, même dans les cas où la fraude est punissable en tant qu'infraction grave, la condamnation ne reflète pas nécessairement cette gravité.

II. Catégories de fraude organisée

8. La fraude est une infraction qui englobe des actions et des comportements très divers, commis dans un large éventail de contextes et à l'encontre de diverses victimes. Dans la recherche universitaire, la fraude a été définie au sens large comme « le fait d'obtenir quelque chose de valeur ou de se soustraire à une obligation par la tromperie »[5]. Par conséquent, à la différence d'autres formes d'infraction acquisitive grave, la fraude est commise par la tromperie plutôt que par la force ou la coercition. En outre, la victime et le délinquant sont rarement tenus de se trouver au même endroit au même moment, et de nombreuses fraudes franchissent les frontières nationales et internationales. La fraude figure dans le droit pénal de nombreux pays, bien qu'elle y soit décrite de manières différentes et avec des degrés de spécificité variables[6]. Certaines lois donnent une description générale des comportements qui constituent une fraude, tandis que d'autres renvoient à certaines activités, certains produits ou services qui figurent en bonne place dans les systèmes frauduleux, comme l'usurpation de l'identité d'une autorité ou la manipulation ou l'utilisation non autorisée de données. Certains États ont introduit des législations distinctes pour traiter les différentes facettes des délits de fraude, par exemple la fraude informatique, la fraude au crédit, la fraude aux enchères ou la fraude à l'encontre d'entreprises. Toutefois, certains éléments fondamentaux de la fraude figurent dans la plupart des définitions juridiques, comme l'utilisation, pour obtenir un avantage ou un bénéfice indû, d'une tromperie causant un préjudice à une autre personne ou organisation. Par tromperie, on entend généralement la malhonnêteté, de fausses déclarations, la ruse, le recours à des artifices, des manœuvres frauduleuses, l'abus de confiance ou la dissimulation ou l'omission d'informations. Dans de nombreux cas, le préjudice causé à autrui est implicite dans l'avantage accordé aux délinquants, mais certains évoquent le préjudice causé à autrui en utilisant des termes tels que l'atteinte ou le préjudice aux intérêts financiers d'autrui, une perte injustifiée ou une escroquerie. Le préjudice peut être causé à un particulier, à une entreprise ou à un État.

9. Les méthodes employées, les entités ciblées et les conséquences pour les victimes et les systèmes sont très diversifiées. C'est pourquoi il a été élaboré, pour comprendre la nature de la fraude, une multitude de typologies. Bien qu'il existe d'autres typologies de fraude reconnues aux niveaux national et international, le

---

[4] Michael Levi, « Organized fraud » in *The Oxford Handbook of Organized Crime*, Letizia Paoli, dir. publ. (Oxford, Oxford University Press, 2014).

[5] Grace M. Duffield et Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, nº 199 (Canberra, Institut australien de criminologie, 2001).

[6] Ont été examinées les définitions juridiques données dans 26 pays de 7 régions différentes : Europe et Amérique du Nord ; Amérique latine et Caraïbes ; Afrique du Nord et Asie occidentale ; Afrique subsaharienne ; Asie du Sud et Asie centrale ; Asie de l'Est et du Sud-Est ; Australie et Nouvelle-Zélande.

présent document d'information se concentre sur la fraude qui vise des individus ou des institutions publiques ou privées dans le but d'obtenir un avantage financier ou un autre avantage matériel. Pour illustrer cela, il a été retenu les grandes catégories suivantes, qui seront explicitées plus en détail dans les sections suivantes du document : a) la fraude sur les produits et services de consommation ; b) la fraude à l'investissement de consommateurs ; c) la fraude à l'emploi ; d) la fraude aux relations et à la confiance ; e) la fraude impliquant l'usurpation de l'identité de fonctionnaires ; f) l'usurpation d'identité ; et g) la fraude à l'encontre d'entreprises ou d'organisations.

10. Dans chaque catégorie, sont mises en évidence les principales formes de tromperie liées à l'avantage ou au résultat escompté par la victime de la transaction frauduleuse. Bien que ces catégories ne soient pas l'apanage des groupes criminels organisés, leur implication accroît considérablement la capacité de commettre des délits et de causer des dommages. Même si chacune représente une technique différente de manipulation des victimes, toutes les catégories peuvent être transnationales et impliquer des coauteurs associés à un groupe criminel organisé. Certaines tromperies sont commises en grand nombre et ont un important effet cumulé, tandis que dans d'autres cas, le préjudice est ressenti de manière aiguë par des groupes de victimes plus restreints.

A. Fraude sur les produits et services de consommation

11. La fraude sur les produits et services de consommation représente l'un des types de fraude les plus répandus, un grand nombre de personnes déclarant avoir été escroquées, ciblées ou exposées à des communications vendant des produits ou services frauduleux. Ce type de fraude implique la vente de produits ou de services qui sont soit inexistants, soit très différents de ce qui est annoncé. Généralement, les fraudeurs commercialisent des produits très demandés ou offrent des produits et des services à un coût inférieur à celui du marché légitime. Certains fraudeurs ciblent leurs publicités sur des groupes considérés comme les plus susceptibles d'être victimes d'un stratagème spécifique. Les fraudes peuvent concerner des vendeurs et des articles entièrement fictifs, mais aussi des entreprises qui présentent sous un faux jour les biens ou les services qu'elles fournissent. Il peut être difficile de confirmer une fraude lorsque le produit ou le service est reçu mais jugé résulter d'une fausse présentation. Parfois, les fraudeurs exploitent le manque d'éducation financière d'une victime pour lui vendre des services financiers tels que des prêts, des plans d'assurance ou des produits de retraite. Il s'agit généralement de produits dont la valeur se situe à terme, les victimes se voyant proposer des projections trop optimistes quant aux performances futures ou les risques n'étant pas correctement expliqués. Les fraudeurs peuvent également omettre de divulguer à la victime les frais, les commissions ou les obligations légales, ce qui peut entraîner des pertes et des pénalités supplémentaires[7].

12. Parmi les produits et services que l'on retrouve souvent dans les fraudes sur les produits et services de consommation, on peut citer les pierres précieuses, les animaux de compagnie, les billets d'événements, les produits médicaux, les loteries ou tirages au sort promettant d'importantes récompenses, ou encore des produits et services financiers tels que des assurances. Cela dit, il existe une variété quasi-infinie de produits et de services qui peuvent être utilisés dans des schémas frauduleux, les fraudeurs cherchant en permanence à s'adapter et à capitaliser sur de nouveaux marchés et sur la demande de consommateurs.

13. Pour commercialiser les produits et services, on utilise différents supports, y compris en ligne. Il s'agit notamment de faux sites Web, de sites d'achat et d'enchères légitimes, de courriers électroniques non sollicités, de courriers postaux

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

ou de ce que l'on appelle des « chaufferies », qui effectuent un grand nombre d'appels de commercialisation et de vente. Certains délinquants profitent du marché dynamique des listes de prospects établies par des moyens légitimes ou illégitimes (tels qu'une violation de données ou une campagne d'hameçonnage en ligne) ou même des répertoires de personnes qui ont été victimes par le passé (listes dites de « suceurs »). Les technologies de l'information et de la communication ont considérablement accru la capacité de commercialiser et de vendre des produits et des services à l'échelle mondiale et à un coût relativement faible. Dans certains cas, c'est le consommateur individuel qui peut perdre de l'argent, mais selon les circonstances et les méthodes employées par les délinquants, ce peut être une plateforme de vente ou un prestataire de services financiers qui subit une perte. Les principales méthodes appliquées sont les suivantes :

a) Faux sites Web créés dans le but de commercialiser et/ou de vendre des produits et des services. Les délinquants peuvent commercialiser le site Web en utilisant des canaux numériques tels que les médias sociaux ou des courriers électroniques non sollicités, ou manipuler les moteurs de recherche Internet pour accroître la probabilité que les personnes qui recherchent des produits ou des services atterrissent sur leur site Web ;

b) Faux vendeurs sur des plateformes légitimes de vente, d'enchères ou de médias sociaux qui utilisent des comptes ouverts avec de fausses identités ou des identités volées. Ces vendeurs exploitent des plateformes légitimes qui donnent accès à un grand nombre d'utilisateurs à la recherche de produits et de services. Par exemple, un groupe criminel organisé a publié des centaines ou des milliers de listes d'articles de grande valeur tels que des automobiles, sur plusieurs sites d'enchères[8].

14. La fraude en ligne qui vise des consommateurs n'a pas besoin d'être élaborée ou complexe. Pour abuser d'un site de vente ou d'enchères légitime, il suffit parfois qu'une seule personne y ouvre un compte et publie une annonce pour vendre un produit inexistant. Toutefois, une partie des délits de fraude à la consommation sont transnationaux et impliquent des groupes criminels organisés. Cette organisation se révèle rarement dans l'échange mené avec la victime, mais plutôt dans la compréhension de la planification et de la préparation qui se cachent derrière. Les principales étapes sont la création et la commercialisation du site Web ou du profil de plateforme, la manipulation de la victime pour maintenir la tromperie (ou obtenir un nouveau paiement) et le transfert de l'argent. Les délinquants adoptent, pour percevoir des paiements tout en laissant une trace financière limitée, diverses méthodes. Celles-ci consistent notamment à convaincre un prestataire de services de paiement que sa société est légitime, à détourner les clients vers de faux sites de paiement, à demander aux victimes de payer à l'aide de cartes de débit prépayées ou à utiliser des comptes de tiers de passeurs de fonds ou des comptes ouverts à l'aide d'identités volées ou falsifiées. Les groupes criminels organisés qui opèrent à partir d'autres pays recrutent généralement des complices dans le pays cible pour faciliter le blanchiment d'argent[9].

B. Fraude à l'investissement

15. La fraude à l'investissement implique généralement la vente d'actions de sociétés, d'obligations ou de devises, certains systèmes commercialisant des

[8] Pour de plus amples informations, voir Office des Nations Unies contre la drogue et le crime (ONUDC), portail de mise en commun de ressources électroniques et de lois contre la criminalité (portail SHERLOC), base de données sur la jurisprudence, *États-Unis d'Amérique* c. *Bogdan Nicolescu, Tiberiu Danet et Radu Miclaus*.
Consultable à l'adresse suivante : https://sherloc.unodc.org/.

[9] Christine Conradt, « Online auction fraud and criminological theories: the Adrian Ghighina case », vol. 6, nº 1, *International Journal of Cyber Criminology*, (janvier/juin 2012) ; et Jack M. Whittaker et Mark Button, « Understanding pet scams: a case study of advance fee and non-delivery fraud using victims' accounts », *Journal of Criminology*, vol. 53, nº 4 (septembre 2020).

investissements dans des biens meubles corporels allant de l'immobilier ou de développements commerciaux à des vins et spiritueux.

16. Pour commettre ces fraudes, il peut falloir bien connaître les contours de la réglementation et les contrôles connexes qui régissent les marchés, la frontière entre pratiques légitimes et illégitimes pouvant être à la fois perméable et difficile à percevoir. Dans certains cas, les délinquants exploitent les mécanismes de confiance en s'enregistrant comme entité réglementée ou en exploitant des acteurs légitimes qui possèdent ce statut. En occupant cette marge grise entre pratiques légitimes et illégitimes, ils entravent l'action des services de détection et de répression ou d'organismes de réglementation qui doivent naviguer et produire des preuves suffisantes et solides d'une tromperie et démontrer qu'une infraction a été commise. En effet, certains peuvent employer des stratagèmes qui, bien que contraires à l'éthique, causent de graves préjudices aux investisseurs mais s'avèrent ne pas être criminels. Les systèmes pyramidaux et de Ponzi sont pour les délinquants un modèle d'activité courant, dans lequel le système d'investissement repose sur l'attraction continue de nouveaux investisseurs pour se maintenir, au lieu de générer des rendements à partir de produits ou d'investissements authentiques, qui n'existent peut-être même pas.

17. La fraude à l'investissement semble être en augmentation, en partie à cause de la hausse des fraudes liées aux investissements dans les cryptomonnaies. Ce nouveau moyen de fraude à l'investissement tire parti de la rapidité et de l'agilité offertes par les espaces numériques, qui permettent aux délinquants de pratiquer une commercialisation de masse rapide et relativement peu coûteuse[10]. Sur de nouveaux marchés financiers tels que celui des cryptomonnaies, les difficultés de réglementation créent des lacunes plus importantes à exploiter. Les méthodes employées dans les fraudes à l'investissement en cryptomonnaies varient en termes de complexité technique et de nouveauté, certaines étant transposées d'autres méthodes telles que la manipulation de marchés et le toilettage financier, qui comprennent la mise en place et la commercialisation de plateformes d'investissement en cryptomonnaies frauduleuses et ce que l'on appelle des « escroqueries de sortie » ou « vols d'investissement », qui consistent à gonfler artificiellement la valeur de jetons frauduleux, qui perdent toute valeur une fois que les délinquants ont retiré tous les fonds investis.

18. Le succès des fraudes à l'investissement dépend de l'efficacité de la communication, qui utilise, pour persuader les investisseurs potentiels, diverses techniques telles que des campagnes de commercialisation ciblées ou de masse ; des techniques de vente agressives ; et la production, pour établir et maintenir la crédibilité et la confiance, de ressources telles que l'image, des sites Web et d'autres supports de commercialisation. Les délinquants peuvent utiliser des canaux de communication spécifiques, ou une combinaison de ceux-ci, qui sont déployés à différents stades du délit. Par exemple, le premier contact avec une victime peut se faire par le biais d'un site Web d'hameçonnage, suivi d'un appel téléphonique de vente, puis d'une poursuite de la manipulation au moyen d'un site Web frauduleux. Les fraudeurs peuvent utiliser, pour entrer en contact avec les victimes, les méthodes suivantes :

a) Télémarketing : à savoir le fait d'utiliser des centres d'appel ou des « chaufferies » pour pratiquer une vente agressive, souvent sous la forme d'appels non sollicités, ciblés au moyen de listes de prospects compilées ou achetées à d'autres acteurs légitimes ou non qui compilent et vendent ces informations personnelles. Dans certains cas, ces listes comprennent des personnes dont on sait qu'elles ont déjà été victimes et qui sont donc vulnérables à des propositions similaires d'investissement, problème dont sont particulièrement victimes les personnes âgées vulnérables. Les centres d'appel peuvent être administrés directement par les auteurs de l'escroquerie

[10] Arianna Trozze, Toby Davies et 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).

ou confiés à des spécialistes capables de fournir ces services de « chaufferie ». Ces centres peuvent être situés à l'étranger par rapport aux victimes, parfois dans des pays connus pour contrôler moins strictement ces activités[11] ;

b) Outils en ligne : certains pays ont connu une importante augmentation des fraudes à l'investissement en ligne, où le premier contact est établi par le biais de communications en ligne telles que des médias sociaux, des sites Web frauduleux et de fausses applications, qui jouent un rôle essentiel dans la tromperie. L'accessibilité des technologies numériques et de vastes ensembles de données sur les consommateurs renforce considérablement la capacité de pratiquer une commercialisation ciblée à grande échelle. Par exemple, des campagnes d'hameçonnage peuvent être utilisées pour attirer et repérer les personnes intéressées par le produit ou le service proposé, ce qui permet de cibler les communications ultérieures. Les auteurs exploitent généralement les médias sociaux et les applications de communication numérique pour commercialiser leurs produits, utilisant parfois l'image de célébrités ou de figures populaires pour persuader les victimes d'investir leur argent. Lorsque ces systèmes frauduleux de cryptomonnaies pénètrent les marchés financiers traditionnels, ils peuvent entraîner de colossales pertes financières ;

c) Contact personnel : les investissements portent souvent sur des sommes importantes qui revêtent une grande signification pour les victimes et, dans certains cas, le contact personnel reste nécessaire pour instiller un niveau de confiance suffisant pour obtenir un investissement. Certains fraudeurs ciblent des victimes avec lesquelles ils entretiennent déjà des relations sociales ou professionnelles afin d'exploiter une confiance déjà existante.

19. Les auteurs de fraudes à l'investissement se donnent beaucoup de mal pour cultiver un vernis de légitimité et adoptent généralement les structures, les processus et le langage d'une organisation légitime formelle, y compris une division claire du travail, avec une hiérarchie et des rôles désignés attribués au personnel. La complexité de l'opération est variable, en fonction de leur motivation à éviter les soupçons ou la détection et à continuer à commettre des délits[12]. Les opérations dites « à l'arraché » peuvent fonctionner pendant une courte période avant de disparaître avec l'argent des investisseurs, tandis que d'autres systèmes peuvent fonctionner sans être détectés pendant de nombreuses années.

20. Parmi les fraudes qui visent les particuliers, ce sont les fraudes à l'investissement qui causent les pertes les plus élevées[13]. Les victimes sont amenées à s'attendre à un rendement financier qui est totalement faux ou grossièrement exagéré. De nombreux investisseurs perdent la totalité ou une grande partie de leur argent. Quelle que soit la méthode employée, les victimes se voient généralement vendre, pour leur investissement, une espérance de valeur à terme, ce qui signifie qu'il peut s'écouler des années après l'investissement initial avant qu'elles ne réalisent qu'elles se sont fait escroquer. Les particularités des différents stratagèmes et la tromperie sous-jacente peuvent varier fortement, mais le résultat en est généralement que les investisseurs perdent la totalité ou une grande partie de leur argent. Exemples :

a) Une tromperie totale dans laquelle le service ou le produit d'investissement n'a jamais existé ;

b) La vente abusive d'actions sans valeur ou surévaluées pour des investissements à haut risque qui ont peu de chances de produire le rendement promis ou peuvent tout simplement échouer ;

---

[11] Neal Shover, Glenn. S. Coffe et Clintin R. Sanders, « Dialing for dollars: opportunities, justifications, and telemarketing fraud », *Qualitative Sociology*, vol. 27, nº 1 (mars 2004).

[12] Michael Levi, « Organized fraud and organizing frauds: unpacking research on networks and organization », *Criminology and Criminal Justice*, vol. 8, nº 4 (décembre 2008).

[13] Voir également Ministère de la justice des États-Unis, « Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes », communiqué de presse, 3 avril 2023.

c) Des techniques de manipulation du marché qui gonflent artificiellement la valeur d'investissements pour des investisseurs peu méfiants.

21. L'importance du préjudice financier subi par les victimes dépend de leur situation financière ou personnelle. Elle peut également dépendre des méthodes employées par les délinquants, par exemple s'ils ciblent l'épargne retraite de personnes, ce qui peut avoir un impact considérable sur une victime[14], alors que certains investissements en cryptomonnaies peuvent être ciblés pour générer des montants plus faibles, mais provenant d'un plus grand nombre de victimes. Dans le cas des victimes de systèmes pyramidaux et de Ponzi, les personnes qui investissent et retirent de l'argent à un stade précoce peuvent ne pas perdre d'argent. Une fois l'argent volé, la victime peut être à nouveau victime du même délinquant ou d'autres délinquants, qui, se prétendant parfois relever d'un organisme légitime, affirment être en mesure de retrouver et de récupérer les fonds perdus, mais demandent à la victime de payer une avance, procédé que l'on qualifie de fraude au recouvrement.

C. Fraude à l'emploi

22. La fraude à l'emploi consiste en la commercialisation massive d'offres d'emploi fausses ou trompeuses sur des sites Web d'offres d'emploi. L'utilisation d'offres d'emploi en ligne s'est considérablement développée dans le secteur légitime, en particulier depuis la pandémie de COVID-19, les recruteurs proposant des modalités de travail plus souples et des possibilités de travail à domicile. Les fraudeurs exploitent la demande de postes convoités, en particulier dans les segments de la population où les occasions légitimes de ce type sont limitées en raison de qualifications ou de formations insuffisantes ou d'un manque d'emplois disponibles dans l'économie locale[15]. Il ressort de la recherche que ce sont généralement les demandeurs d'emploi les moins à l'aise financièrement ou en situation désespérée qui sont la cible de ces fraudeurs.

23. Ces fraudes consistent généralement à publier en ligne une offre d'emploi qui est soit totalement fictive, soit bien moins rentable que ce qui est annoncé. Il peut s'agir, par exemple, de publicités pour des opportunités d'affaires, de travail à domicile ou de mannequinat. Dans certains cas, les fraudeurs demandent aux victimes des paiements anticipés avant de prendre position ; les raisons invoquées sont multiples : dossiers de démarrage, voyages, formation ou vérification de la solvabilité. Le résultat est souvent que la victime perd de l'argent sans recevoir l'emploi promis. Dans d'autres cas, les fraudeurs envoient des chèques contrefaits aux victimes pour payer leurs frais de démarrage, avant de prétendre avoir effectué un paiement de trop et de demander à la victime de rembourser le délinquant. La victime perd l'argent viré et se retrouve avec le coût du chèque une fois qu'il a été décelé comme étant contrefait.

24. Les fraudeurs à l'emploi peuvent également être motivés par le vol de données personnelles que les victimes fournissent lors du processus de candidature, ce qui les expose à une victimisation ultérieure. Dans certains cas, le travail s'avère être de nature criminelle. Par exemple, la victime peut être amenée à faciliter un blanchiment d'argent (en tant que mule) ou à servir de coursier pour livrer des articles achetés frauduleusement (en cas d'usurpation d'identité). Dans les cas les plus graves, la victime devient l'objet d'une traite à visée de travail forcé et de criminalité forcée[16].

---

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

[15] Alexandrea J. Ravenelle, Erica Janko et 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, nº 7 (juillet 2022), p. 1591 à 1610 ; et Delali Kwasi Dake, « Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites », *International Journal of Computer Applications*, vol. 184, nº 51 (mars 2023).

[16] Pour plus d'informations sur ces deux formes d'exploitation, voir également le *Rapport mondial sur la traite des personnes 2002* (publications des Nations Unies, 2022), ainsi que l'ONUDC,

D. Fraude aux relations et à la confiance

25. Le processus d'établissement de la confiance joue un rôle essentiel dans tout type de fraude. Toutefois, dans le cas de la fraude aux relations et à la confiance, les délinquants favorisent et exploitent le pouvoir des relations personnelles en développant la confiance nécessaire pour manipuler et tromper les victimes, parfois à de multiples reprises. Dans ce type de fraude, la victime ne s'attend pas à recevoir un produit ou un service, mais plutôt à nouer une véritable relation avec le délinquant. La complexité de ces fraudes réside moins dans l'exploitation de systèmes techniques ou technologiques que dans la dynamique de la relation entre la victime et l'auteur du délit.

26. De nombreux fraudeurs établissent des relations en ligne et utilisent des techniques d'ingénierie sociale pendant des mois, voire des années, pour gagner la confiance de la victime. Les victimes s'attendent généralement à une relation romantique, mais cela peut prendre d'autres formes, comme une amitié de confiance, ou même le désir d'une relation avec un membre de la famille de la victime. Plusieurs études ont identifié, au sein de la population vieillissante et âgée, des vulnérabilités liées à des facteurs tels que la solitude, l'isolement social et le désir de nouer de nouvelles relations. Les criminels ciblent et exploitent cette vulnérabilité par le biais d'un processus d'amitié ou de séduction. En outre, les délinquants peuvent se faire passer pour un parent ou un ami en grande difficulté et ayant besoin d'argent pour remédier à une situation. Ces fraudes peuvent être ciblées et incorporer des détails personnels tirés de messages publiés par l'ami ou le parent sur les médias sociaux afin de rendre la communication avec la victime plus crédible. Ces communications se font généralement par SMS. Il existe des exemples d'intelligence artificielle utilisée pour cloner la voix d'un parent ou d'un ami lors d'un appel téléphonique.

27. L'un des principaux éléments de cette catégorie de fraude est la fraude amoureuse, par laquelle les délinquants construisent des relations amoureuses en ligne dans le but de tromper et d'extorquer de l'argent à leurs victimes. Pour ces dernières, les pertes financières peuvent être considérables. Il s'agit d'un problème qui sévit dans de nombreuses régions du monde et qui tire parti de la croissance des réseaux sociaux en ligne et, plus particulièrement, d'une tendance sociétale plus large à trouver des relations amoureuses en ligne. La première approche des victimes se fait généralement sur les médias sociaux ou des sites et applications de rencontres par un délinquant qui utilise une fausse identité et un profil correspondant. Un même délinquant peut passer d'une identité à l'autre pour cibler et séduire une victime potentielle. Une fois la relation établie, le délinquant peut obtenir de la victime un avantage financier en lui demandant d'abord une petite somme d'argent avant de demander des sommes plus importantes, souvent en évoquant un scénario de crise qui permet de faire pression sur la victime (par exemple, une urgence médicale ou un besoin urgent de voyager). Si des images sexuelles ont été échangées, de l'argent peut également être extorqué à la victime.

28. Dans un cas plus récent d'application de cette méthode, on a vu la fraude à l'idylle converger avec la fraude à l'investissement dans des cryptomonnaies. Dans l'escroquerie au romantisme ou la fraude au « dépeçage » (terme dont l'utilisation n'est pas recommandée par respect pour les victimes), un délinquant entretient une relation personnelle avec une victime en ligne. Au lieu de fabriquer un scénario de crise, il exploite la relation d'intimité et de confiance pour attirer la victime dans un système d'investissement frauduleux. Pour le délinquant, cela peut inclure des étapes supplémentaires de planification et de préparation, y compris l'élaboration d'un site Web ou d'une application frauduleuse accessible à la victime, voire la fourniture d'un « service client » pour les investisseurs [17]. L'intégration d'investissements en

« Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: policy report » (Bangkok, 2023).

[17] Cassandra Cross, « Romance baiting, cryptorom and "pig butchering": an evolutionary step in romance fraud », *Current Issues in Criminal Justice* (2023) ; et Fangzhou Wang et Xiaoli Zhou,

cryptomonnaies dans la tromperie a un certain nombre de conséquences : elle étend le groupe de victimes potentielles à des groupes d'âge plus jeunes ; introduit les victimes dans un marché peu familier, volatile et à haut risque, ce qui signifie qu'elles sont moins susceptibles de se reconnaître comme victimes ; et rend encore plus difficile, pour les enquêteurs, la tâche de remonter jusqu'aux délinquants.

29. La recherche sur la fraude à l'idylle s'est davantage concentrée sur les victimes et leur expérience que sur les délinquants, qui sont moins visibles. Cette fraude est considérée comme relevant généralement de la criminalité transnationale pratiquée par des groupes criminels organisés, avec une certaine concentration dans certaines régions. En ce qui concerne la fraude au « dépeçage », certains groupes criminels organisés ont adopté des structures plus élaborées, semblables à celles d'une entreprise, dans lesquelles il existe une division claire du travail (par exemple, contact avec les victimes, technologie de l'information et blanchiment d'argent) et le recrutement d'une main-d'œuvre composée de personnes ayant besoin d'argent et susceptibles d'être exploitées, y compris dans le cadre de la traite d'êtres humains[18].

30. Quelles que soient les caractéristiques des victimes, les conséquences d'une fraude aux relations et à la confiance peuvent être considérables. Outre des pertes financières, les victimes souffrent d'une rupture de confiance et de la perte d'une relation personnelle importante. En outre, elles subissent un préjudice psychologique et émotionnel important. Certaines peuvent même refuser d'admettre qu'elles sont ou ont été victimes d'une fraude.

E. Fraude impliquant l'usurpation de l'identité de fonctionnaires

31. La fraude impliquant l'usurpation de l'identité de fonctionnaires, ou fraude à l'usurpation d'identité, consiste à manipuler des communications de manière à ce qu'elles semblent provenir d'un fonctionnaire ou d'un autre représentant officiel, que ce soit de la police, de l'administration fiscale, d'une banque ou d'un service gouvernemental. Cette fraude utilise toute une série de prétextes et de scénarios, tels que l'usurpation de l'identité d'une administration fiscale ou d'un autre service gouvernemental qui réclame une dette impayée ; un message d'un banquier affirmant que l'argent sur un compte bancaire est menacé par des criminels ; ou un message de la police qui prétend avoir détecté une infraction pénale commise par la victime.

32. L'une des principales caractéristiques de cette fraude est le recours à des techniques de persuasion qui font moins appel aux désirs et besoins des victimes (comme dans le cas des fraudes à la consommation) et évoquent plutôt la peur, la crainte, l'angoisse et l'inquiétude. En induisant un état émotionnel élevé, on empêche la prise de décision et l'on rend les victimes plus susceptibles d'être manipulées. Ces messages menacent la victime d'une issue négative, y compris d'une forme de réponse juridique, si elle n'envoie pas de paiement ou ne transfère pas de fonds.

33. Cette fraude implique généralement des communications de masse telles que des courriers électroniques non sollicités ; des communications à l'aide des médias sociaux ; des SMS ; ou des appels téléphoniques automatisés, qui diffusent un message enregistré. Ces technologies permettent d'entrer en contact quasi-simultané avec des milliers de victimes à la fois, ce qui leur confère une portée immense.

F. Usurpation d'identité

34. L'usurpation d'identité[19] consiste à utiliser des informations d'identité volées ou fausses pour obtenir un accès direct à des biens, à des services ou à de l'argent de

---

« 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, nº 5 (2023).

[18] ONUDC, « Casinos, cyber fraud, and trafficking in persons ».

[19] Voir également *Handbook on Identity-related Crime* de l'ONUDC (disponible en anglais seulement) (Vienne, 2011).

victimes, par exemple en utilisant des informations volées pour effectuer des achats ou accéder à des comptes financiers. Elle peut être perpétrée sans communication directe ni action de la part de la personne dont l'identité est usurpée, car la cible est souvent le fournisseur des biens, des services ou de l'argent. Ainsi, le préjudice est réparti entre les différentes victimes, y compris celle dont l'identité est usurpée, le prestataire de services financiers ou toute autre entreprise dont les fonds sont exfiltrés et, dans certains cas, le fournisseur des biens ou des services achetés avec les fonds volés.

35. Il existe, en ce qui concerne l'identité, différentes formes d'informations qui peuvent être acquises, chacune d'elles pouvant être exploitée de différentes manières. Il s'agit notamment des informations personnelles, qui comprennent les identités numériques des individus dans différents environnements en ligne, comme le nom ou la date de naissance ; les données relatives aux comptes financiers, comme les numéros de cartes de crédit ; les informations relatives aux comptes en ligne, y compris les noms d'utilisateur et les mots de passe ; et des données biométriques telles qu'une empreinte digitale volée sur un appareil électronique.

36. Les délinquants peuvent accéder à ces informations en s'introduisant dans le système ; en utilisant des systèmes d'ingénierie sociale tels que des campagnes d'hameçonnage classique ou par texto ; ou en accédant à des marchés criminels en ligne qui vendent les données. Les données peuvent être utilisées pour acheter des biens et des services, soumettre des demandes de prêts et d'autres financements ou accéder aux comptes des victimes pour en transférer de l'argent. Cette méthode se caractérise, en outre, par ce qui suit :

a) Intrusion dans le système : certains fraudeurs pratiquent l'acquisition d'informations personnelles au moyen de techniques illicites de piratage, de déploiement de logiciels malveillants ou d'hameçonnage ;

b) Marchés criminels en ligne : il existe, en ce qui concerne l'achat et la vente d'informations sur l'identité, une économie souterraine dynamique qui peut être exploitée par les usurpateurs d'identité. La possibilité d'acquérir des informations de cette manière supprime certains obstacles techniques pour les fraudeurs qui, autrement, ne disposeraient pas de ces capacités pour voler des informations personnelles ;

c) Ingénierie sociale : il s'agit souvent d'une publicité ou d'une autre communication non sollicitée envoyée par courrier électronique ou autre communication en ligne, SMS ou appel téléphonique non sollicité, par lesquels les victimes sont amenées à fournir des informations personnelles. Le degré de sophistication varie, mais des méthodes plus complexes telles que l'usurpation de sites Web légitimes peuvent conduire à une compromission plus importante en donnant aux délinquants un accès direct à des comptes en ligne.

37. Il existe toute une série de techniques employées par les délinquants pour usurper une identité. Parmi les principales, on peut citer la prise de contrôle de comptes, la fraude à la carte et la fraude à la demande, qui sont définies comme suit :

a) Prise de contrôle de comptes : dans ce type de fraude, les auteurs obtiennent des identifiants légitimes pour accéder à des comptes d'utilisateurs. Il peut s'agir de comptes bancaires, mais aussi d'autres types de comptes financiers (par exemple, des fournisseurs de monnaie virtuelle), de sites de vente au détail ou de tout fournisseur de biens et de services. Le compte peut être utilisé à diverses fins, notamment pour transférer directement des fonds vers des comptes contrôlés par les délinquants ou pour acheter frauduleusement des biens ou des services. Dans certains cas, l'acquisition des informations permettant d'accéder au compte d'une victime constitue la première d'une série d'étapes nécessaires pour accéder à l'argent, aux biens ou aux services au moyen d'intrusions ultérieures dans le système. Cela peut nécessiter de surmonter des mesures de sécurité telles que l'authentification à deux facteurs. Par conséquent, les délinquants recourent à des techniques supplémentaires telles que l'échange de cartes SIM et d'autres méthodes de paiement ;

b) Fraude à la carte : achats non autorisés effectués à distance auprès d'un vendeur, soit en ligne, soit par téléphone. L'acquisition des références financières d'une victime suffit pour tromper à la fois le fournisseur de services financiers et le vendeur commercial sans qu'il soit nécessaire d'interagir directement avec la victime ou d'accéder à la carte de paiement physique. Généralement, les usurpateurs d'identité doivent, pour exploiter les références financières d'une victime, suivre un certain nombre d'étapes clefs :

i) acquérir des connaissances, des ressources et des références financières sur les marchés criminels en ligne ;

ii) dissimuler les commandes pour éviter de déclencher les algorithmes de détection des fraudes sur un site commercial ;

iii) réceptionner les commandes à une adresse qui ne permette pas de remonter jusqu'aux délinquants ;

iv) revendre les articles à titre individuel ou les vendre en gros en se faisant passer pour un commerçant légitime sur les principales places de marché en ligne ;

c) Fraude à la demande : ces fraudes exploitent la disponibilité généralisée d'informations personnelles et les utilisent pour demander un crédit au nom de la victime. Cela se fait généralement dans le but d'obtenir un prêt auprès d'un prestataire de services financiers. Pour pouvoir usurper l'identité d'une personne de manière crédible, les délinquants doivent accéder à un ensemble d'informations personnelles (par exemple, le nom, l'adresse ou la date de naissance). L'une des tendances émergentes consiste à utiliser la technologie pour créer des identités synthétiques en combinant des identifiants réels et des identifiants fabriqués. Une fois établies, ces identités peuvent être cultivées au fil du temps pour que l'on puisse, devenu plus solvable, solliciter des produits financiers de grande valeur.

38. Il est à noter que l'usurpation d'identité n'exige pas l'implication de groupes criminels organisés. Cependant, la capacité de commettre ce délit à grande échelle et de réaliser d'importants profits est considérablement accrue par les compétences et les ressources dont dispose le crime organisé. Cette menace revêt une acuité particulière avec la prolifération de cibles en ligne disponibles dans des économies de plus en plus numériques. La manipulation et l'usurpation d'identité peuvent, dans l'activité criminelle organisée, remplir diverses fonctions, notamment empêcher de remonter jusqu'aux auteurs[20].

G. Fraude à l'encontre d'entreprises ou d'organisations

39. La fraude à l'encontre d'entreprises ou d'organisations consiste généralement à abuser de systèmes internes ou d'une relation commerciale pour escroquer la victime. Cette fraude peut être commise par une personne interne ou externe à l'organisation. Elle peut être commise, sans résulter nécessairement de stratagèmes conçus d'emblée pour commettre une fraude, par des entreprises et des acteurs par ailleurs légitimes ou utilisant des produits légitimes, parfois en réponse à des pressions internes ou à des pratiques ou à une culture de travail douteuses.

40. Exemples de fraude à l'encontre d'entreprises ou d'organisations :

a) La fraude par compromission du courrier électronique d'entreprise est une fraude informatique perpétrée à grande échelle. Des entreprises et des organisations de toutes tailles et de tous secteurs sont victimes de ce type de fraude, généralement commise par des délinquants externes. Les délinquants s'infiltrent dans les systèmes et utilisent des techniques d'ingénierie sociale pour persuader le personnel d'effectuer des transferts de fonds non autorisés vers des comptes contrôlés par les premiers. Les

[20] Simon Baechler, « Document fraud: will your identity be secure in the twenty-first century? », *European Journal on Criminal Policy and Research*, vol. 26, nº 3 (juin 2020).

pertes subies par les victimes peuvent être très élevées. La première étape consiste à infiltrer les systèmes de communication d'une organisation pour persuader les destinataires qu'on est légitime. Les principales méthodes consistent à pirater les comptes de courrier électronique de membres du personnel ; à envoyer des courriels d'hameçonnage pour obtenir le détail des comptes des membres du personnel ; ou à exploiter des prestataires de services de communication pour usurper des noms de domaine connus de l'organisation cible [21]. Les délinquants adoptent différents stratagèmes, exploitant notamment une relation existante entre deux entreprises en émettant une fausse facture ; en envoyant un courrier électronique prétendument émis par un cadre supérieur et présentant une demande urgente de fonds ; ou en se faisant passer pour un avocat demandant un virement bancaire pour traiter une affaire sensible[22]. La communication peut s'étaler sur une certaine période, les délinquants pouvant prendre du temps pour comprendre l'organisation et ses systèmes et les victimiser à plusieurs reprises ;

b) Les fraudes aux états financiers comprennent une multitude de moyens par lesquels des professionnels par ailleurs légitimes d'un marché financier induisent en erreur et faussent la perception d'autres personnes telles que des investisseurs, des régulateurs et d'autres acteurs du marché quant à la santé financière et aux perspectives d'avenir d'une entreprise ou d'un fonds. Des types de fraude comptable similaires peuvent également dissimuler le détournement d'actifs, la mauvaise utilisation ou le détournement de fonds. Ces fraudes peuvent être commises en réponse à des pressions exercées pour répondre à des attentes de performance. Il peut s'agir, par exemple, de dirigeants d'entreprise, de traders malhonnêtes ou de gestionnaires de fonds spéculatifs qui rendent compte de leurs performances financières. Dans certains cas, l'impact de ces fraudes se fait sentir au-delà de l'entreprise, y compris dans d'autres entreprises et secteurs, voire dans l'ensemble de l'économie[23] ;

c) Les fraudes à long ou court terme peuvent être commises par des sociétés commerciales existantes ou par des sociétés qui peuvent avoir été achetées ou créées dans un but frauduleux. Ces entreprises créent des antécédents de crédit, une confiance ou une crédibilité qui sont utilisés pour tromper un acheteur, un vendeur ou un créancier et l'amener à fournir des biens ou un financement. Elles agissent ainsi sachant qu'elles ne peuvent pas payer ou qu'elles n'ont pas l'intention de le faire.

III. Questions à examiner

41. Le Groupe de travail souhaitera peut-être faire porter ses délibérations sur les thèmes suivants :

a) Nature de la fraude organisée dans différents pays ;

b) Utilisation qui pourrait être faite de la Convention contre la criminalité organisée pour prévenir et combattre la fraude organisée, et conférer à la fraude le caractère d'infraction grave, telle que définie à l'article 2 de la Convention ;

c) Possibilités de coopération internationale efficace, y compris avec le secteur privé ;

---

[21] Norah Saud Al-Musib *et al.*, « Business email compromise (BEC) attacks », *Materials Today: Proceedings*, [vol. 81, Partie 2 (2023)] ; et Geoffrey Simpson, Tyler Moore et Richard Clayton, « Ten years of attacks on companies using visual impersonation of domain names », document de recherche présenté au Symposium on Electronic Crime Research (eCrime), organisé par le Groupe de travail sur la lutte contre le hameçonnage et tenu à Boston (États-Unis d'Amérique) du 16 au 19 novembre 2020.

[22] Alessandro E. Agazzi, « Business Email Compromise (BEC) and cyberpsychology ». Consultable à l'adresse suivante : https://arxiv.org/ ; et Al-Musib *et al.*, « Business email compromise (BEC) attacks ».

[23] Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serious Fraud Office, « Senior bankers sentenced to 9 years for rigging EURIBOR rate », 1er avril 2019.

d) Échange d'informations sur la prévention de la fraude organisée, la protection des victimes, des témoins et des lanceurs d'alerte, la poursuite des groupes criminels pratiquant la fraude organisée, ainsi que la promotion de partenariats à ces fins ;

e) Recensement des besoins d'assistance technique à satisfaire en rapport avec la mise en œuvre de la Convention contre la criminalité organisée pour prévenir et combattre la fraude organisée.

IV. Suite à donner et recommandations possibles

42. Le Groupe de travail souhaitera peut-être faire les recommandations suivantes :

a) Encourager les États parties qui ne l'ont pas encore fait à envisager de conférer à la fraude le caractère d'infraction grave, telle que définie au paragraphe b) de l'article 2 de la Convention contre la criminalité organisée, afin de faire en sorte que, lorsque l'infraction est de nature transnationale et implique un groupe criminel organisé, une coopération internationale efficace puisse être mise en place en vertu de la Convention ;

b) Exhorter les États parties à utiliser les outils offerts par la Convention contre la criminalité organisée pour élaborer ou modifier leur législation nationale, s'il y a lieu, pour prévenir et combattre la fraude, y compris la fraude commise par des groupes criminels organisés ;

c) Encourager les États parties à analyser, en consultation avec d'autres parties concernées, lorsqu'il y a lieu, l'évolution des activités des groupes criminels organisés en matière de fraude organisée et à partager ces informations et données avec l'Office des Nations Unies contre la drogue et le crime ;

d) Demander à l'Office des Nations Unies contre la drogue et le crime, sous réserve de la disponibilité de ressources extrabudgétaires, de recueillir, d'analyser et de diffuser des informations concernant la fraude organisée ;

e) Exhorter les États parties à s'accorder mutuellement la coopération internationale la plus large possible, y compris l'entraide judiciaire, dans le cadre des enquêtes, des poursuites et des procédures judiciaires relatives à la fraude organisée et aux infractions connexes couvertes par la Convention contre la criminalité organisée et les protocoles y afférents ;

f) Encourager les États parties à renforcer leur coopération avec les parties concernées, y compris le secteur privé, les organisations de la société civile, les médias, les universités et la communauté scientifique, afin de prévenir et de combattre la fraude organisée, notamment par des campagnes d'éducation et de sensibilisation ;

g) Demander à l'Office des Nations Unies contre la drogue et le crime, sous réserve de la disponibilité de ressources extrabudgétaires, de continuer d'élaborer des outils d'assistance technique et de fournir aux États parties qui le demandent une telle assistance, y compris en matière de renforcement des capacités, qui les aide à appliquer efficacement la Convention contre la criminalité organisée pour prévenir et combattre la fraude organisée ;

h) Demander aux États parties qui ne l'ont pas encore fait de mettre à jour leurs dossiers législatifs relatifs à l'incrimination de la fraude organisée dans le portail de mise en commun de ressources électroniques et de lois contre la criminalité (portail SHERLOC).