

Conséquences de la crise du Covid-19 en matière de blanchiment de capitaux et de financement du terrorisme

La crise actuelle liée à la pandémie du Covid-19 place notre société face à des défis inconnus. Les autorités nationales ont comme priorité principale d'avoir le contrôle de la situation sur le plan médical mais cherchent, par ailleurs, à limiter autant que possible l'ampleur et les conséquences de la crise économique qui en découle. Bien que la situation actuelle soit sans précédent, des crises moins importantes ont démontré par le passé que les criminels s'adaptent très rapidement à des circonstances économiques changeantes et extrêmes, répondant à la devise « never waste a good crisis ». Les rapports publiés par Europol¹, Interpol² et le GAFI³ montrent que les groupes criminels ont rapidement saisi l'occasion d'exploiter la crise liée au coronavirus en adaptant leurs modes opératoires existants ou en se livrant à de nouvelles activités criminelles.

Le but poursuivi par la CTIF dans la présente note est de sensibiliser les déclarants aux conséquences à court terme qu'a la situation actuelle sur les formes de criminalités sous-jacentes au blanchiment, se manifestant actuellement en particulier en matière d'escroquerie. Sur la base des études effectuées par les organisations internationales et du travail d'analyse de ses propres dossiers, la CTIF a identifié des typologies concrètes destinées à aider les déclarants à détecter ces formes d'escroqueries et, ensuite, à enrichir la présente note sur la base des déclarations.

Les fraudes analysées touchent majoritairement la vente de matériel utilisé pour lutter contre le coronavirus et contre la propagation de la maladie COVID-19. Les produits concernés sont notamment des masques de protection et des (prétendus) médicaments contre le virus et la maladie. Dans la suite de cette note, ces produits sont désignés comme « matériel COVID-19 ».

La présente note contient donc certains indicateurs. Un indicateur, pris isolément, n'éveille pas forcément de soupçon. La présence de plusieurs des comportements repris ci-dessous devrait toutefois engendrer une vérification de la transaction.

Nous invitons les déclarants à nous signaler tout potentiel lien avec la crise du coronavirus en reprenant le terme "COVID19" dans le champ prévu pour la motivation dans le système de déclaration en ligne de la CTIF.

¹ <https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic>

² <https://www.interpol.int/>

³ <https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html>

1. Escroqueries dirigées contre des sociétés

a. Modes opératoires

En matière d'escroqueries dirigées contre des sociétés, on distingue fréquemment deux modes opératoires:

- La crise du coronavirus est prise comme prétexte pour détourner des paiements
- Des criminels se font passer pour des producteurs et distributeurs de matériel COVID-19

La crise du coronavirus est prise comme prétexte pour détourner des paiements

Les fraudes au président et BEC sont désormais bien connues et de nombreuses campagnes de prévention ont été menées pour lutter contre ce phénomène. Les criminels tirent profit de la situation créée par la crise, dont le confinement et les difficultés économiques, pour passer en dessous du radar de vigilance mis en place au sein des sociétés visées.

Voici deux exemples :

- Des criminels se font passer pour le dirigeant d'une société et contactent l'établissement financier de celle-ci. Le prétendu dirigeant explique que toute son entreprise est désorganisée et qu'il travaille à partir de son domicile. Il argumente qu'il ne saurait dès lors suivre les procédures usuelles (notamment de contresignature). Il va insister sur une communication qui passe exclusivement par e-mail.

- En tirant encore prétexte de la désorganisation d'une entreprise, des criminels argumentent que les paiements ne se font désormais plus sur les comptes centraux de la société, mais directement sur les comptes des sites de production. Ils peuvent notamment tirer argument de problèmes de trésorerie et de problèmes avec leur service comptable. Ce stratagème permet de détourner des paiements – effectués dans le cadre d'une relation d'affaires existante – sur des comptes frauduleux.

Du côté de la sécurité informatique, le travail à domicile crée de nouveaux risques. Des criminels peuvent exploiter ces failles pour gagner un accès à des documents confidentiels, utilisés par la suite dans le cadre de fraudes sophistiquées. Il faut rappeler que le vol d'informations privilégiées est une des raisons du succès des fraudes au président et BEC

Des prétendus producteurs et distributeurs de matériel COVID-19.

En se servant de l'ingénierie sociale, des criminels se font passer pour des vendeurs de matériel COVID-19. La situation d'urgence constante dans laquelle des acteurs du secteur privé et public peuvent se trouver pour acquérir ce matériel crée une vulnérabilité accrue.

Afin de donner crédit à leur offre, des criminels vont notamment :

- Produire de faux documents
- Créer des sites Internet fictifs
- Créer des sociétés écran
- Se faire passer pour des entreprises sérieuses qui produisent effectivement le matériel en question.

b. Indicateurs relatifs aux victimes

- *'Nouveau' compte bénéficiaire*

Le client entretient des relations d'affaires avec un certain nombre de cocontractants. Soudainement, il entend effectuer un virement :

- En faveur d'un nouveau bénéficiaire et / ou
- En faveur d'un compte ouvert dans un pays dans lequel il n'exerce pas d'activité.

L'établissement financier doublera de vigilance lorsqu'un paiement effectué vers un nouveau bénéficiaire est rapidement suivi d'un nouvel ordre de transfert. En effet, les fraudeurs forts de leur premier succès ont tendance à procéder à un nouvel ordre de virement

- *Incohérences relatives à un nouveau bénéficiaire*

Les incohérences suivantes peuvent notamment apparaître en lien avec le bénéficiaire :

- Le bénéficiaire est une société écran
- Le bénéficiaire est un nouvel acteur sur le marché et n'a pas d'expérience documentée dans le commerce de matériel COVID-19
- Le bénéficiaire n'est pas le producteur du matériel, mais un tiers qui n'a pas de relation documentée avec le producteur
- Le bénéficiaire n'a pas d'activité économique propre
- Le compte bénéficiaire est situé dans une juridiction qui n'a pas de lien apparent avec la transaction à effectuer

- *Caractère urgent de la transaction*

Le client insiste sur l'urgence de la transaction à effectuer. Cette attitude peut faire suite à la pression exercée sur le client par le criminel, qui explique qu'en l'absence de paiement immédiat, sa marchandise – très convoitée – sera envoyée à un autre client.

- *Noms de domaines frauduleux*

Les instructions de virement proviennent d'un compte de messagerie ressemblant étroitement au compte de messagerie du client. L'adresse de messagerie a toutefois été légèrement modifiée en ajoutant, en modifiant ou en supprimant un ou plusieurs caractères.

Les instructions peuvent également provenir de la bonne adresse e-mail du client mais qui a été piratée. Ces cas de fraude sont plus sophistiqués.

- *Incohérences relatives à la documentation*

Les pièces justificatives remises au professionnel peuvent présenter des incohérences. En premier lieu, les messages échangés entre le client et son prétendu cocontractant peuvent présenter des signes pointant vers du phishing.

La documentation consultée par la CRF montre aussi que les criminels créent des sites Internet fictifs pour simuler une activité économique en lien avec la vente de matériel COVID-19. L'expérience de la CRF montre que les conditions générales de tels sites ne sont souvent pas cohérentes par rapport à la prétendue activité économique. Le niveau de détail des explications fournies sur des sites fictifs reste également très limité.

c. Indicateurs relatifs aux auteurs

- *Incohérences relatives au montant de la transaction*

Les montants perçus par le titulaire du compte bénéficiaire peuvent être incohérents par rapport au profil du client. Dans les affaires analysées par la CRF, des personnes ont ainsi reçu des montants de plusieurs dizaines de milliers d'euros, alors qu'elles ne bénéficiaient que d'un salaire modeste. De tels comptes sont souvent ouverts par des 'money mules'.

- *Incohérences relatives à l'activité du client*

Le client a ouvert un compte pour recevoir des salaires d'un employeur local et reçoit des montants importants de l'étranger, sans lien avec l'exécution d'un contrat de travail.

Exemple:

Le client est salarié d'une entreprise et reçoit un virement de 25.000 EUR d'une entreprise française, avec comme objet du virement « Paiement de la facture 123456 ».

L'objet des ordres de virement perçus témoigne d'une incohérence par rapport à l'activité professionnelle du client.

Exemple :

Une société a été constituée avec un objet social très général et perçoit soudainement des sommes d'argent en lien avec la vente de matériel COVID-19.

2. Escroqueries dirigées contre des particuliers

Les cas étudiés se rapportent à l'escroquerie et aux infractions à la propriété intellectuelle. Les schémas criminels sont classiques :

- Du matériel COVID-19 est mis en vente, mais jamais livré
- Du matériel contrefait est vendu
- La vente de médicaments en dehors des réseaux autorisés

La commission de ces fraudes se fait essentiellement en ligne. A côté des places de marché qui peuvent être exploitées à cet effet, l'envoi de publicités par e-mail (SPAM) ou la publication d'annonces sur les réseaux sociaux est fréquente. Pour plus de détails, il est renvoyé aux notes d'Europol, d'Interpol et du GAFI reprises ci-dessus.

Les éléments suivants peuvent constituer des indicateurs d'une escroquerie:

- *Indicateurs relatifs à la nature des produits mis en vente*

Les termes suivants peuvent notamment être utilisés lors de la vente de matériel Covid-19:

- COVID-19
- Coronavirus
- SARS-CoV-2
- Masque
- Mask
- FFP2
- FFP3
- "(personal) protective equipment" ou "PPE"
- Chloroquine - Hydroxychloroquine - Azithromycine
- Plaquenil
- Hand sanitizer
- Désinfectant
- Alcohol 70%
- Ethanol 70%
- Face shield
- Hazmat suits
- Decontamination suits

- Ventilator, respirator, or breathing machine
- Respiratoire artificiel
- Appareil respiratoire

- *Indicateurs relatifs aux prix de l'objet*

Des prix anormalement bas ou élevés par rapport à ceux pratiqués usuellement.

- *Indicateurs relatifs au bénéficiaire de la transaction*

Le bénéficiaire est une société écran ou le bénéficiaire n'est pas actif dans la distribution de matériel COVID-19.

- *Indicateurs relatifs au canal de distribution*

La vente de produit se déroule en-dehors du canal de distribution normal.
