PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

Note - Faux virements

Analyse des typologies

Version 1.0 du 24.04.2019

Ce document est destiné aux professionnels soumis la loi modifiée du 12 novembre 2004 concernant la lutte contre le blanchiment et contre le financement du terrorisme et plus particulièrement aux établissements financiers définis par cette loi.

Bureaux :
41B boulevard Franklin D. Roosevelt
L-2450 Luxembourg

Adresse postale :
L-2080 Luxembourg

Courriel : crf@justice.etat.lu
Internet : www.crf.lu
Téléphone : (+352) 47 59 81-447

TABLE DES MATIERES

Introduction 2

1 Typologies 2

1.1 La fraude au président (*CEO fraud*) 2

1.2 Les fausses factures 3

1.3 « L'attaque de l'homme du milieu » (« *man in the middle attack* ») 3

1.4 L'utilisation de courriels piratés 3

2 Indicateurs 4

2.1 Les indicateurs d'application générale 4

2.1.1 Le montant du virement 5

2.1.2 Les money mules 5

2.1.3 Informations antérieures 5

2.2 Indicateurs s'appliquant au compte de la victime 5

2.2.1 Compte bénéficiaire incohérent 6

2.2.2 « Nouveau » compte bénéficiaire 6

2.2.3 Comportement inhabituel du client 6

2.3 Indicateurs s'appliquant au compte de l'auteur 7

2.3.1 Incohérence du montant de la transaction 8

2.3.2 Incohérence par rapport à l'activité du client 8

2.3.3 Transactions subséquentes 8

3 Que faire en cas de virement exécuté ou tenté ? 8

3.1 Le professionnel détient le compte de la victime 8

3.1.1 Le virement a été exécuté 8

3.1.2 Le virement n'a pas été exécuté 9

3.2 La réaction de la victime 9

3.2.1 Informer son établissement financier 9

3.2.2 Déposer une plainte pénale 9

3.3 Le professionnel détient le compte du suspect 10

3.3.1 S'abstenir d'exécuter des opérations sur le compte 10

3.3.2 Faire une déclaration à la CRF 10

3.3.3 Déposer une plainte pénale 10

3.3.4 Coopérer avec les autorités 10

4 Liens utiles 11

4.1 Police Grand-Ducale 11

4.2 Europol 11

4.3 Interpol 11

INTRODUCTION

Au cours des dernières années, la Cellule de Renseignement Financier (ci-après : la CRF) a constaté une forte augmentation des déclarations liées aux faux ordres de virement. Du fait de l'exposition internationale de la place financière, la CRF s'est engagée dans une coopération internationale systématique avec ses homologues étrangers, qui a abouti à la création d'un groupe de travail dans le cadre du Groupe EGMONT[1].

La mise en commun de l'expérience des CRF impliquées dans ce groupe de travail a mis en exergue que :

- La vigilance des professionnels soumis à la loi modifiée du 12 novembre 2004 concernant la lutte contre le blanchiment et contre le financement du terrorisme (ci-après : la Loi de 2004) apporte les meilleurs résultats dans la prévention et la lutte contre les faux ordres de virement ;
- Pour les virements exécutés, une action dans les 72 heures suivant l'exécution du virement est cruciale pour avoir une chance réaliste de récupérer les fonds escroqués.

Concernant ce deuxième point, le groupe de travail EGMONT a mené un important travail de sensibilisation des CRF à travers le monde, afin d'assurer une coopération internationale efficace.

La présente analyse contient :

- Un aperçu des typologies constatées (1),
- Une liste des indicateurs à appliquer par les professionnels soumis à la Loi de 2004 (2),
- Des indications à suivre en cas de fraude exécutée ou tentée (3).

1 TYPOLOGIES

1.1 LA FRAUDE AU PRÉSIDENT (*CEO FRAUD*)

L'auteur contacte (soit par courriel soit par téléphone) le service comptabilité d'une entreprise, en se faisant passer pour le PDG ou un membre de la direction de celle-ci. Tout en insistant sur le caractère confidentiel de l'entretien, il donne des explications sur un important contrat qui devrait être conclu dans la plus grande urgence.

L'auteur est généralement très bien informé sur la structure de l'entreprise visée et se sert de nombreuses pièces falsifiées préparées à l'avance pour justifier de la réalité et du sérieux de l'opération.

Pièces à l'appui, le fraudeur arrive à convaincre le comptable d'exécuter un virement en faveur d'un compte à l'étranger.

Très souvent, les auteurs n'agissent pas seuls mais en bande organisée : l'un se fera passer pour le PDG du groupe, l'autre pour l'avocat s'occupant de la transaction, voire le notaire instrumentant. Dans certains cas d'espèce, les fraudeurs n'ont pas hésité à se faire passer pour des autorités étatiques ou internationales, notamment pour persuader les établissements financiers de ne pas clôturer leur relation d'affaires avec le client afin de pouvoir continuer à recevoir le produit d'autres escroqueries en cours ou consommées.

L'employé qui ne s'est pas rendu compte de la tromperie sera parfois sollicité à faire des virements additionnels. Dans la plupart des affaires, le comptable ne s'est en effet rendu compte de la supercherie que plusieurs jours après les faits.

[1] http://www.egmontgroup.org

Les analyses menées par la CRF ont mis en évidence que les fonds escroqués sont souvent transférés vers un premier compte tenu auprès d'une banque européenne, puis répartis sur un ou plusieurs autres compte(s) dans des pays tiers. Ce morcellement des virements permet aux fraudeurs de maximiser leurs chances de mettre à l'abri au moins une partie des fonds escroqués.

1.2 LES FAUSSES FACTURES

Le schéma classique consiste à envoyer de fausses factures au service comptabilité d'une société. Plusieurs variations dans les méthodes utilisées ont pu être constatées :

- Les auteurs se renseignent sur les cocontractants de l'entreprise visée, en faisant notamment des recherches sur Internet. Ces informations leur permettent d'émettre de prétendues factures au nom du cocontractant de l'entreprise, en indiquant leur propre numéro de compte ou celui d'un complice.
- Les auteurs s'introduisent dans le système informatique de l'entreprise visée ou de son cocontractant pour trouver les contrats en cours, avec les plans de paiement approuvés. Ces informations supplémentaires leur permettent d'émettre de prétendues factures – d'une qualité quasiment parfaite – au moment opportun et pour les montants renseignés dans la comptabilité.
- Dans la continuité des deux méthodes décrites ci-dessus, les auteurs prennent connaissance de factures qui ont réellement été émises par le cocontractant de la société visée. Sous différents prétextes – notamment en se faisant passer pour une société d'affacturage – ils arrivent à persuader le comptable de verser la somme due sur un autre compte en banque.

Les exemples repris ci-dessus sont donnés à titre purement illustratif. Les méthodes utilisées varient constamment.

1.3 « L'ATTAQUE DE L'HOMME DU MILIEU » (« *MAN IN THE MIDDLE ATTACK* »)

Les auteurs interceptent les communications électroniques entre deux sociétés, sans que celles-ci ne s'en rendent compte. Ils peuvent utiliser cette méthode pour acquérir une information parfaite sur les relations existantes entre deux parties. Dans ce schéma classique, ils émettent par la suite de fausses factures (voir point 2.2).

L'attaque peut toutefois s'avérer plus sophistiquée, en ce que les auteurs ne se limitent pas à intercepter les messages, mais se mettent à les modifier. Ils peuvent donc introduire de fausses informations dans un échange réel entre deux cocontractants voire dans un futur contrat à signer.

A titre d'exemple, on peut citer l'insertion de fausses informations bancaires ou l'indication de faux délais de paiement pour camoufler l'infraction.

1.4 L'UTILISATION DE COURRIELS PIRATÉS

Les fraudeurs piratent des comptes e-mail divers afin d'amener des institutions financières à exécuter des ordres de virement non autorisés par les ayants droits sur le compte au moyen de diverses techniques :

a) Envoyer directement des ordres de virement aux institutions financières en exerçant une pression psychologique sur leurs employés par voie d'e-mails et de documents de support relatifs au transfert requis pour en justifier la cause ;

b) Impressionner les employés de la société victime de la fraude en leur soumettant des instructions pour exécuter des ordres de virement relatifs à des transactions urgentes en falsifiant ou créant des emails internes ayant une apparence légitime[2] ;
c) Pirater le compte e-mail des intermédiaires financiers tels que des courtiers afin de transmettre de faux ordres de virement aux institutions financières et ce au nom du client commun vers un compte détenu par le fraudeur ;
d) Pirater le compte e-mail des prestataires de services professionnels tels que des avocats ou sociétés fiduciaires afin de transmettre de faux ordres de virement aux institutions financières vers un compte détenu directement par le fraudeur.

2 INDICATEURS

Le client, victime d'une escroquerie sophistiquée, ne se rend souvent pas compte du caractère frauduleux du virement effectué. L'ingénierie sociale *(angl. social engineering)* employée par les auteurs, l'a mis en confiance et l'empêche de se poser des questions sur la légitimité du transfert exécuté.

Dans la plupart des affaires analysées par la CRF, le client n'a informé sa banque ou déposé une plainte auprès de la police ou du parquet que plusieurs jours après les faits. Or, les chances de récupérer les fonds plusieurs jours après l'exécution du virement tendent vers zéro. Les premières 24 heures sont cruciales pour envisager de recouvrer les fonds. Une intervention dans les 72 heures peut parfois encore aboutir à un résultat satisfaisant.

Seule une vigilance accrue des transactions du client par l'établissement financier concerné est susceptible de parer à l'absence de réaction de la part du client.

Il est primordial que l'établissement financier prenne en compte l'ordre de virement reçu au vu du profil type du client, de l'historique des virements effectués sur le compte et des circonstances qui entourent l'ordre de virement en lui-même afin de prévenir, identifier et arrêter une tentative de faux virement ou afin de permettre une réaction rapide pour en réduire les conséquences le cas échéant.

Pour aider le professionnel dans cette tâche, le groupe de travail EGMONT a dressé une liste non exhaustive d'indicateurs permettant de déceler des virements frauduleux. Un indicateur, pris isolément, n'éveille pas forcément de soupçon. La présence de plusieurs des comportements repris ci-dessus devrait toutefois engendrer une vérification – voir un blocage en interne – de la transaction.

En cas de doute quant à la légitimité d'un ordre de virement, la CRF ne peut que fortement recommander aux établissements financiers de procéder à des vérifications et des investigations internes additionnelles afin de respecter leurs obligations professionnelles avant l'exécution d'un tel virement. Dans la mesure où l'ingénierie sociale est l'une des clés de voûte du système mis en place par les auteurs de faux virements, les établissements financiers sont invités à contacter des interlocuteurs différents au sein de l'établissement client.

Nous avons subdivisé nos indicateurs en trois catégories, applicables

- à tous les comptes,
- au compte de la victime,
- au compte de l'auteur.

2.1 LES INDICATEURS D'APPLICATION GÉNÉRALE

[2] Il peut être précisé qu'en cas d'instructions ou confirmations écrites, de la part d'une personne interne ou externe à l'entreprise, les auteurs vont parfois jusqu'à copier de façon très minutieuse le style de langage habituellement utilisé. Dans les cas les plus sophistiqués, ces imitations peuvent être très élaborées et résulter d'un véritable travail d'observation préalable, notamment à travers d'intrusions dans le système informatique de la victime.

2.1.1 LE MONTANT DU VIREMENT

Par opposition aux fraudes classiques, les typologies décrites sous le point 1) portent généralement sur des montants élevés. Ce constat s'explique par le fait que les victimes sont majoritairement des sociétés et que les auteurs fondent leur demande de virement sur des factures émises en contrepartie de l'exécution de contrats importants.

Il n'est pas rare que le virement porte sur des sommes dépassant 100.000 ou même un million d'euros.

2.1.2 LES MONEY MULES

Les auteurs de faux virements ont souvent recours à des intermédiaires, les « *money mules* ». D'après Europol, un *« money mule »* est une personne qui transfère des fonds obtenus illégalement entre différents comptes bancaires ou autres, très souvent dans différents pays, pour le compte d'autrui. Les mules sont ainsi recrutées par les criminels pour recevoir de l'argent sur leur compte bancaire, afin de le retirer ou de le transférer sur des comptes détenus à l'étranger, souvent en contrepartie d'une commission[3].

Dans le cas des « *money mules »*, les montants faisant l'objet de faux virements ne sont généralement pas cohérents par rapport au profil du client. L'établissement financier doit notamment s'interroger sur l'origine des fonds et l'objet économique du transfert.

Par exemple :

Le compte du client X qui travaille comme assistante maternelle et perçoit un salaire de 2.800 euros tous les mois est crédité de 100.000 euros avec mention « paiement facture n° xxxxx ». Ce virement ne correspond pas au profil du client.

2.1.3 INFORMATIONS ANTÉRIEURES

L'établissement peut déjà avoir pris connaissance de comptes bénéficiaires utilisés dans le cadre de faux ordres de virement, notamment en raison de réclamations d'autres clients.

2.2 INDICATEURS S'APPLIQUANT AU COMPTE DE LA VICTIME

Les auteurs connaissant souvent l'activité et les contrats en cours de leur victime, de sorte qu'ils veillent à demander des ordres de virement similaires à ceux normalement opérés par le client. Dans les cas analysés par la CRF, le montant de la transaction – pris isolément – n'a pas éveillé de soupçon chez le professionnel.

En revanche, le compte bénéficiaire du virement peut constituer un indicateur fiable d'un faux ordre de virement. Au moindre soupçon, la CRF recommande aux établissements financiers de vérifier la légitimité de l'ordre de virement projeté avec leur client.

Le comportement du (prétendu) client peut également éveiller un soupçon chez l'établissement financier de la victime.

[3] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

2.2.1 COMPTE BÉNÉFICIAIRE INCOHÉRENT

L'ordre de virement s'inscrit dans une relation d'affaires existante. Le client décide toutefois d'effectuer un virement sur un compte appartenant prétendument au même bénéficiaire, mais qui n'a encore jamais été utilisé auparavant.

2.2.2 « 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 dans la foulée.

2.2.3 COMPORTEMENT INHABITUEL DU CLIENT

2.2.3.1 URGENCE OU CONFIDENTIALITÉ DE LA TRANSACTION

Le client insiste sur l'urgence et/ou la confidentialité de la transaction. Le temps jouant de toute évidence en faveur de l'auteur, il est fréquent que celui-ci exerce de la pression sur le client pour bénéficier d'une exécution rapide du virement.

La confidentialité de la transaction est invoquée pour éviter tout contrôle en interne de la légitimité du transfert. Le comptable est ainsi mis dans l'impossibilité de vérifier l'authenticité de la transaction demandée.

2.2.3.2 NON-RESPECT DU PRINCIPE DES QUATRE YEUX

Le client applique normalement le principe des quatre yeux (double signature) pour tous les transferts impliquant des sommes importantes. Pour une raison quelconque, ce principe ne devrait pas s'appliquer à la transaction en question. Dans certains cas, l'employé du client produit des pièces pour confirmer sa position.

2.2.3.3 STYLE D'ÉCRITURE INHABITUEL

Bien que ce constat soit assez rare dans le cadre des typologies présentées dans ce document, il arrive que les pièces justificatives

- contiennent de nombreuses fautes d'orthographe,
- ne soient pas conformes à la charte graphique utilisée habituellement par le client ou son cocontractant,
- soient envoyées à des horaires qui ne sont pas ceux auxquels l'établissement financier reçoit habituellement des instructions de virement du client,
- le style de langage ne correspond pas à celui qu'est utilisé habituellement par le client.

2.2.3.4 INCOHÉRENCES PAR RAPPORT À LA DOCUMENTATION FOURNIE ANTÉRIEUREMENT OU UTILISATION DE FAUX

Dans le cadre de l'exécution de contrats importants, une documentation a déjà été remise par le client à l'établissement financier. L'ordre de virement n'est notamment pas conforme aux échéances de paiement ou aux montants y repris.

2.2.3.5 NOMS DE DOMAINE FRAUDULEUX – PHISHING/PHARMING

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.

> Exemples :
> contact@abc.com au lieu de contact@abc.lu
> contact@adc.com au lieu de contact@abc.com

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

2.2.3.6 INSTRUCTIONS D'UN NOUVEL EMPLOYÉ DU CLIENT

Les instructions de virement émanent d'un employé du client qui est une nouvelle personne habilitée sur le compte ou une personne habilitée qui n'a pas envoyé d'instructions de virement dans le passé.

2.2.3.7 INSTRUCTIONS QUE PAR VOIE ÉLECTRONIQUE

Les auteurs favorisent souvent les échanges écrits par e-mail. Dans certains cas, ils ont avancé différents prétextes pour ne pas entrer en contact avec l'établissement financier de la victime, qui voulait notamment demander des précisions.

2.3 INDICATEURS S'APPLIQUANT AU COMPTE DE L'AUTEUR

Le comportement du titulaire du compte bénéficiaire constitue fréquemment un indicateur fiable pour identifier des faux ordres de virement. Pour mieux comprendre le fonctionnement des comptes bénéficiaires, il est également renvoyé aux développements effectués au sujet des « *money mules* » exposés au point 2.1.2 ci-dessus. La CRF insiste sur le fait qu'en cas de soupçon, le professionnel ne saurait exécuter la transaction[4].

[4] *« Les professionnels sont tenus de s'abstenir d'exécuter toute transaction qu'ils savent, soupçonnent ou ont des motifs raisonnables de soupçonner d'être liée à un blanchiment, à une infraction sous-jacente associée, ou à un financement du terrorisme avant d'en avoir informé la Cellule de renseignement financier conformément aux paragraphes 1er et 1bis et de s'être conformés à toute instruction particulière émanant de la Cellule de renseignement financier »* (article 5, 3 de la Loi de 2004).

2.3.1 INCOHÉRENCE DU 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.

2.3.2 INCOHERENCE PAR RAPPORT A L'ACTIVITE 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.

Par exemple :

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

2.3.3 TRANSACTIONS SUBSEQUENTES

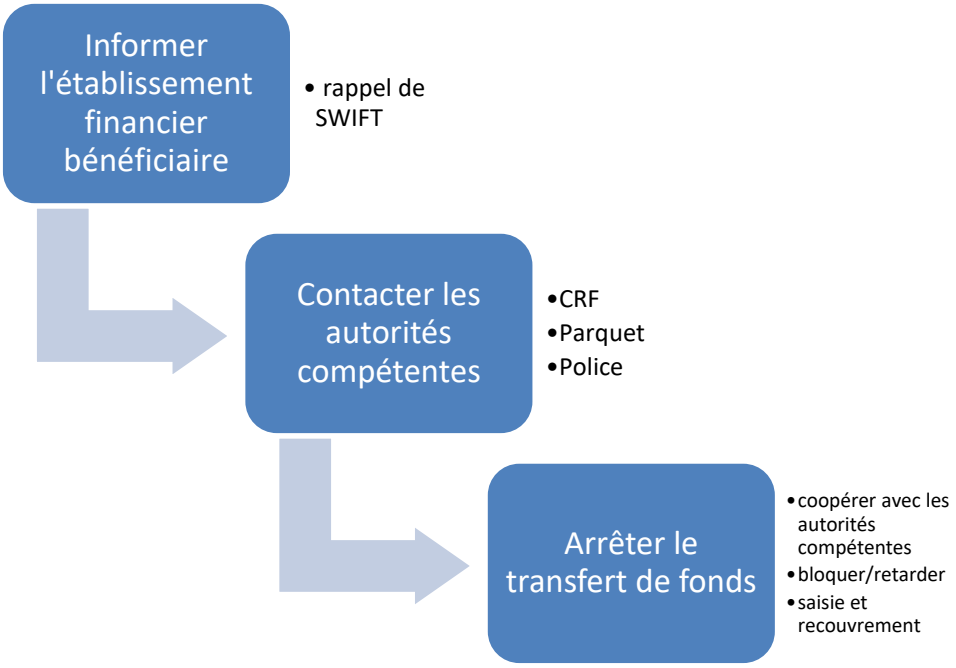
Le titulaire du compte bénéficiaire veut transférer les fonds reçus sur un ou plusieurs autres comptes, respectivement veut faire des retraits en espèces.

3 QUE FAIRE EN CAS DE VIREMENT EXÉCUTÉ OU TENTÉ ?

3.1 LE PROFESSIONNEL DÉTIENT LE COMPTE DE LA VICTIME

3.1.1 LE VIREMENT A ÉTÉ EXÉCUTÉ

Un seul mot d'ordre – réagir rapidement. Plus rapide sera la réaction, plus les chances de recouvrement des fonds seront élevées.



3.1.1.1 INFORMER L'ÉTABLISSEMENT FINANCIER BÉNÉFICIAIRE

Dans l'hypothèse où le virement a déjà été exécuté, l'établissement financier de la victime d'un faux virement informe immédiatement **l'établissement financier bénéficiaire des fonds** du virement en question.

Cette information peut notamment se faire par SWIFT recall.

Conformément aux accords interbancaires, l'établissement financier du bénéficiaire peut être autorisé à refuser les fonds et les retourner sur le(s) compte(s) d'origine.

3.1.1.2 FAIRE UNE DÉCLARATION À LA CRF

Après avoir informé l'établissement financier bénéficiaire, le professionnel fait immédiatement une déclaration d'opération suspecte (DOS) à la CRF.

Si l'exécution du virement a été faite depuis moins de 72 heures, le professionnel :

- Peut faire une première DOS sommaire, renseignant avec précision toutes les informations sur la ou les transaction(s) suspecte(s), ainsi qu'une motivation en quelques mots. Le professionnel s'oblige à fournir tout détail supplémentaire dans les 24 heures.
- Contacte la CRF par téléphone après avoir envoyé la DOS (le cas échéant sommaire).

3.1.1.3 DÉPOSER UNE PLAINTE PÉNALE

Le dépôt d'une plainte auprès de la police ou du parquet est à envisager par la victime et/ou l'établissement financier. Nous recommandons fortement le dépôt d'une plainte par la victime.

3.1.2 LE VIREMENT N'A PAS ÉTÉ EXÉCUTÉ

Il est demandé au professionnel de faire une DOS à la CRF, même si le virement n'a pas été exécuté et est donc resté au stade de la tentative. Cette déclaration permettra à la CRF de dénoncer le compte – potentiellement à risque élevé – à la CRF du pays concerné.

3.2 LA REACTION DE LA VICTIME

3.2.1 INFORMER SON ÉTABLISSEMENT FINANCIER

La victime doit immédiatement contacter son établissement financier, afin de permettre à celui-ci de suivre la procédure décrite au point 3.1. ci-dessus.

3.2.2 DÉPOSER UNE PLAINTE PÉNALE

Il est très fortement recommandé de déposer une plainte à la police ou au parquet.

Si l'exécution du virement a été faite depuis moins de 72 heures, la victime doit insister sur l'urgence présentée par sa plainte.

3.3 LE PROFESSIONNEL DETIENT LE COMPTE DU SUSPECT

3.3.1 S'ABSTENIR D'EXÉCUTER DES OPÉRATIONS SUR LE COMPTE

L'établissement financier bénéficiaire, qui a un soupçon de virement frauduleux, ne doit pas exécuter de transactions pouvant aboutir à une perte des fonds sur le compte[5].

Ce soupçon peut notamment être motivé par :

- Une analyse interne (en prenant notamment en compte les indicateurs repris sous le point 2.3. ci-dessus),
- Une information de l'établissement financier de la prétendue victime.

3.3.2 FAIRE UNE DÉCLARATION À LA CRF

Le professionnel doit immédiatement faire une déclaration d'opération suspecte (DOS) à la CRF. La CRF décidera d'un ordre de blocage conformément à article 5 (3) de la Loi de 2004.

Si les fonds ne sont plus sur le compte, l'établissement financier doit fournir toute information sur la destination suivante des fonds (notamment le ou les nouveau(x) compte(s) bénéficiaire(s)).

3.3.3 DÉPOSER UNE PLAINTE PÉNALE

Le dépôt d'une plainte auprès de la police ou du parquet est à envisager par l'établissement financier.

3.3.4 COOPÉRER AVEC LES AUTORITÉS

L'établissement financier doit coopérer avec les autorités compétentes, notamment pour :

- Répondre à des demandes d'information de la CRF – demande 5 (1) b),
- Exécuter un ordre de blocage,
- Exécuter une perquisition,
- Exécuter une saisie judiciaire.

[5] *« Les professionnels sont tenus de s'abstenir d'exécuter toute transaction qu'ils savent, soupçonnent ou ont des motifs raisonnables de soupçonner d'être liée à un blanchiment, à une infraction sous-jacente associée, ou à un financement du terrorisme avant d'en avoir informé la Cellule de renseignement financier conformément aux paragraphes 1er et 1bis et de s'être conformés à toute instruction particulière émanant de la Cellule de renseignement financier »* (article 5, 3 de la Loi de 2004).

4 LIENS UTILES

4.1 POLICE GRAND-DUCALE

CyberScams: Sensibilisation aux escroqueries financières en ligne les plus courantes :
https://police.public.lu/fr/actualites/2018/10/w42/17-cyberscams.html

4.2 EUROPOL

Fraud scams targeting employees :
https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees

4.3 INTERPOL

Social engineering scams:

https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams