



MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité



FLASH DGSi #92

MARS 2023

INGÉRENCE ÉCONOMIQUE

RISQUES D'ESCROQUERIES PAR DES ACTEURS SE
PRÉSENTANT COMME DES FONDS
D'INVESTISSEMENT



Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne. Il est également disponible sur le site internet : www.dgsi.interieur.gouv.fr

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

securite-economique@interieur.gouv.fr



RISQUES D'ESCROQUERIES PAR DES ACTEURS SE PRÉSENTANT COMME DES FONDS D'INVESTISSEMENT

Les sociétés qui rencontrent des difficultés financières ou les start-up qui lèvent des fonds peuvent être sollicitées par des fonds d'investissement étrangers formulant des propositions financières attractives.

Des acteurs se présentent parfois comme des fonds d'investissement étrangers, en utilisant des identités fictives ou en usurpant des identités réelles. Ils exposent les entreprises qu'ils ciblent à d'importants risques financiers et d'atteinte à leur réputation et à leurs savoir-faire.

PREMIER EXEMPLE

Des individus usurpent l'identité d'un fonds d'investissement étranger dans le but d'escroquer une entreprise française.

Une société française a lancé une campagne de levée de fonds en communiquant sur les réseaux sociaux professionnels et la presse spécialisée. Un fonds d'investissement étranger a pris attache avec la société pour lui proposer un prêt sous forme d'obligations convertibles aux conditions très avantageuses, en contrepartie duquel il a uniquement été demandé à la société française la création d'un fonds commun de créance¹ dans le pays d'origine de l'investisseur pour procéder au transfert des fonds.

L'entreprise française s'est étonnée qu'aucune autre demande particulière n'ait été formulée par le fonds avant l'opération, notamment la réalisation d'un audit de la société. Les soupçons de la société ont été renforcés lorsque les représentants du fonds ont refusé de communiquer par visio-conférence.

Souhaitant vérifier l'honorabilité du fonds d'investissement, l'entreprise française a alors constaté qu'un message de prudence apparaissait sur le site internet du fonds indiquant qu'il ne contactait jamais les entreprises directement. La société française a pris conscience qu'elle avait été victime d'une tentative

¹ Special purpose vehicle en anglais, il s'agit d'un véhicule de financement dont le seul objectif est d'acquérir les créances selon une procédure simplifiée.

d'escroquerie et que des individus avaient usurpé l'identité du fonds d'investissement en créant des adresses de messagerie électronique dont le libellé était proche de celles du fonds d'investissement.

DEUXIÈME EXEMPLE

Une start-up française placée en redressement judiciaire après avoir été victime d'une escroquerie menée par un fonds d'investissement étranger fictif.

Une start-up française a lancé une levée de fonds de plusieurs millions d'euros. Elle a été contactée par un fonds d'investissement étranger qui, après plusieurs échanges par téléphone et par courrier électronique, a annoncé vouloir participer à la levée de fonds. Le dirigeant de la société française a été invité à se déplacer dans le pays du fonds d'investissement pour signer le contrat de financement.

Une fois sur place et alors que le dirigeant de la start-up devait être reçu par les investisseurs, les représentants du fonds ont prétexté une indisponibilité et ne se sont jamais présentés. Ils ont toutefois invité la société française à s'acquitter de plusieurs types de frais, en espèces et par virement bancaire.

Le fonds d'investissement s'était ensuite engagé à partager une partie de certaines dépenses administratives avant de signaler à la start-up qu'une institution bancaire avait fait opposition à son virement. À la demande du fonds, la société française s'est donc acquittée du restant de ces frais à un agent de recouvrement indiqué par le fonds étranger.

Face à cette multiplication des demandes de versements, la start-up s'est rapprochée des services de l'État qui lui ont indiqué qu'il s'agissait d'une escroquerie élaborée par un fonds d'investissement fictif, établi dans un paradis fiscal avec une domiciliation commune à de nombreuses autres entreprises, et que les individus avaient en parallèle usurpé l'identité d'employés de réelles structures financières étrangères. Ayant subi un préjudice financier de plusieurs dizaines de milliers d'euros et n'ayant pas pu récupérer les sommes versées, la start-up française a été placée en redressement judiciaire.

COMMENTAIRES

Lorsque les entreprises victimes d'escroqueries sont des structures de petite taille, les conséquences de telles démarches sur leur stabilité financière peuvent être importantes, jusqu'à remettre en cause leur pérennité. Les start-up et petites entreprises sont rarement dotées de directions juridiques ou financières à même de les conseiller ou de détecter des indices d'une escroquerie.

Dans certains cas, la combinaison d'usurpations d'identités réelles et de création de fausses structures peut rendre l'identification de l'escroquerie difficile à déceler.

Outre le préjudice financier qui peut être subi par les entreprises victimes d'escroqueries, ces situations peuvent ralentir un processus de levée de fonds, rendre la société vulnérable à propositions financières peu avantageuses ou à des tentatives d'ingérence d'acteurs étrangers intéressés par leurs savoir-faire ou technologies.

Par ailleurs, ce type d'escroqueries peut amener les entreprises à communiquer des données stratégiques, qui pourraient être utilisées au profit de concurrents.

PRÉCONISATIONS DE LA DGSi

BONNES PRATIQUES À ADOPTER POUR SE PRÉMUNIR DES ESCROQUERIES

- **Avoir un usage prudent des réseaux sociaux, même professionnels.** Les réseaux sociaux sont une source d'information pour les individus mal intentionnés. Il est recommandé d'être prudent sur la nature des informations partagées et de faire preuve d'une vigilance renforcée vis-à-vis des approches réalisées exclusivement par le biais des réseaux sociaux.
- **Se renseigner sur l'honorabilité de l'investisseur.** Des vérifications élémentaires peuvent être réalisées par l'entreprise, à commencer par une lecture attentive du site Internet de l'investisseur, une consultation des profils des dirigeants et une vérification de sa domiciliation.
- **Privilégier les rencontres physiques préalablement à tout engagement et, à défaut, exiger au moins un échange en visio-conférence.** Lors d'échanges dématérialisés, une vigilance particulière doit être portée au nom de domaine employé par ses interlocuteurs et à sa bonne concordance avec le nom de l'entreprise qu'ils disent représenter. Un refus des interlocuteurs de toute rencontre ou de se présenter par le biais d'une visio-conférence doit être un élément d'alerte à prendre en compte.
- **Appliquer les procédures de façon stricte, sans dérogation.** Les acteurs malveillants cherchent à tirer profit de la méconnaissance des procédures juridiques et financières internationales de jeunes entreprises pour leur porter atteinte. Il est impératif de se renseigner sur les procédures locales et de ne pas céder à des impératifs d'urgence qui pourraient être avancés par ses interlocuteurs. L'application stricte des procédures permet d'éviter le paiement de frais supplémentaires.
- **Plusieurs services de l'État peuvent être sollicités afin de s'assurer de l'honorabilité d'un interlocuteur financier :** réseau des délégués à l'information stratégique et à la sécurité économiques (DISSE), directions régionales de l'économie, de l'emploi, du travail et des solidarités (DREETS), réseau international de la direction générale du Trésor implanté à l'étranger, etc. La DGSi peut également être sollicitée.

EN CAS D'IDENTIFICATION D'UNE ESCROQUERIE

- **Mettre fin aux échanges avec le partenaire.** Mettre rapidement un terme aux échanges lors d'une tentative d'escroquerie permet de limiter son exposition aux risques de captation de données et d'atteinte à la réputation.
- **Sensibiliser ses salariés.** Sensibiliser en priorité les services chargés de la gestion juridique et financière de l'entreprise, mais aussi l'ensemble des salariés, afin de limiter les risques liés à d'éventuelles approches directes des acteurs malveillants auprès d'autres interlocuteurs dans l'entreprise.
- **Signaler les faits à la DGSi.** Particulièrement lorsqu'elles se manifestent dans le cadre d'une levée de fonds, ces escroqueries peuvent cibler plusieurs entreprises stratégiques sur une même

période de temps. La DGSi pourra sensibiliser en retour ses interlocuteurs aux risques présentés par un acteur identifié comme malveillant.

- **Déposer plainte auprès des services locaux de police ou de gendarmerie.** Même en l'absence de tout préjudice, cette démarche permet de signaler ces agissements, de procéder à des recoupements et d'identifier ainsi leurs auteurs en caractérisant leurs modes opératoires. En cas de préjudice, elle sera le préalable à toute procédure d'indemnisation engagée auprès des banques ou assureurs. Il est conseillé de joindre aux déclarations tous les éléments justificatifs (journaux de connexions, messageries échangées, coordonnées bancaires) permettant de prouver l'escroquerie.

