AVIS IMPORTANT : TENTATIVES DE FRAUDE PAR USURPATION D'IDENTITE

Comme de nombreuses sociétés, nous observons une recrudescence des tentatives de fraude utilisant abusivement le nom, l'identité visuelle ou les coordonnées de notre société, notamment à travers la création de faux noms de domaine visant à tromper la vigilance de l'interlocuteur, et, dans certains cas, celles d'anciens collaborateurs sur des applications de messagerie instantanée.

Ces démarches ont pour objectif d'induire en erreur des investisseurs en leur proposant de faux produits financiers, de fausses opportunités d'investissement ou en tentant d'obtenir des informations personnelles ou bancaires.

Nous vous recommandons d'être vigilants pour vous protéger et vous rappelons que :

- Notre site web officiel est https://www.comgest.com.
- Les réseaux sociaux et applications de messagerie instantanée (telles que WhatsApp) ne sont pas utilisés comme moyen de contact par Comgest.

➢ Fraude et usurpation d'identité

La fraude désigne un acte intentionnel de tromperie ou de dissimulation visant à obtenir un avantage indu au détriment d'autrui. Elle recouvre un large ensemble de comportements déloyaux, tels que l'usurpation d'identité lorsqu'elle est employée à des fins malveillantes.

L'usurpation d'identité consiste à s'approprier sciemment l'identité d'une personne physique ou morale, ou à utiliser ses éléments d'identification (nom, logo, adresse email, documents officiels) dans le but de tromper un tiers. Lorsqu'elle vise à obtenir un avantage indu ou à causer un préjudice, l'usurpation d'identité constitue une forme de fraude et peut également relever de l'escroquerie.

➢ Quels réflexes adopter pour se protéger d'une fraude ?

- Considérez avec la plus grande vigilance toute prise de contact non sollicitée par téléphone, email, SMS, réseaux sociaux ou applications de messagerie instantanée. Quelle qu'en soit la forme (téléphone, courrier, email ou message), les usurpations sont fréquentes, nombreuses et faciles à réaliser.

- Ne communiquez aucune information personnelle (téléphone, mail, pièces d'identité, RIB, IBAN, justificatifs de domicile…) via un site web ou par téléphone à une personne prétendant nous représenter, sans avoir vérifié leur authenticité par le biais de nos canaux officiels.

- Renseignez-vous sur la société dont votre interlocuteur se revendique en recherchant ses coordonnées officielles (téléphone, adresse mail et postale) via d'autres sources afin de vérifier la véracité des informations fournies et n'hésitez pas à vérifier l'identité de vos

interlocuteurs via l'envoi d'un email ou un appel aux numéros téléphoniques indiqués sur les sites officiels.

- Si un message vous semble provenir d'une source inconnue ou douteuse, veillez à ne pas cliquer sur les liens ni à ouvrir les pièces jointes et n'y répondez pas.

Pour plus de recommandations, nous vous invitons à consulter les informations pédagogiques mises en ligne par l'Autorité des Marchés Financiers en France ou par votre régulateur local.

➢ Que faire si vous pensez avoir été victime d'une fraude ?

1. Si cette fraude est en rapport avec Comgest, Informez-nous directement à l'adresse info@comgest.com.

2. En cas d'usurpation via WhatsApp, signalez le message, le groupe et ou/le profil suspect comme suit, puis supprimez le message de votre appareil après signalement :
   - Signalement d'un profil : cliquez sur le contact à signaler puis, en bas de page, cliquez sur « Signaler + numéro de téléphone ».
   - Signalement d'un groupe : cliquez sur le nom du groupe en haut des discussions, puis, en bas de page, cliquez sur « Signaler le groupe ».

3. Si vous êtes de nationalité française, effectuez un signalement Pharos (portail officiel du ministère de l'intérieur pour les signalements des contenus illicites de l'Internet) : https://internet-signalement.gouv.fr/.