

BELANGRIJKE MEDEDELING: POGINGEN TOT FRAUDE DOOR IDENTITEITSFRAUDE

Net als veel andere bedrijven zien wij een toename van pogingen tot fraude waarbij misbruik wordt gemaakt van de naam, de visuele identiteit of de contactgegevens van ons bedrijf, met name door het creëren van valse domeinnamen om de waakzaamheid van de gesprekspartner te misleiden, en in sommige gevallen door het gebruik van de namen van voormalige medewerkers op instant messaging-applicaties.

Deze praktijken hebben tot doel beleggers te misleiden door hen valse financiële producten of valse beleggingsmogelijkheden aan te bieden of door te proberen persoonlijke of bankgegevens te verkrijgen.

Wij raden u aan waakzaam te zijn om uzelf te beschermen en herinneren u eraan dat:

- Onze officiële website is <https://www.comgest.com>.
- Comgest maakt geen gebruik van sociale media en instant messaging-apps (zoals WhatsApp) om contact op te nemen.

➤ **Fraude en identiteitsdiefstal**

Fraude is een opzettelijke daad van misleiding of verzwijging met als doel een onrechtmatig voordeel te verkrijgen ten koste van anderen. Het omvat een breed scala aan oneerlijke gedragingen, zoals identiteitsfraude wanneer deze voor kwaadwillige doeleinden wordt gebruikt.

Identiteitsfraude bestaat uit het opzettelijk zich toe-eigenen van de identiteit van een natuurlijke of rechtspersoon, of het gebruik van diens identificatiegegevens (naam, logo, e-mailadres, officiële documenten) met het doel een derde te misleiden. Wanneer identiteitsfraude tot doel heeft een onrechtmatig voordeel te verkrijgen of schade te berokkenen, vormt het een vorm van fraude en kan het ook onder oplichting vallen.

➤ **Hoe kunt u zich tegen fraude beschermen?**

- Wees uiterst waakzaam bij ongevraagde contacten via telefoon, e-mail, sms, sociale netwerken of instant messaging-apps. Ongeacht de vorm (telefoon, post, e-mail of bericht) komen gevallen van identiteitsfraude vaak voor, zijn talrijk en gemakkelijk uit te voeren.
- Geef geen persoonlijke informatie (telefoonnummer, e-mailadres, identiteitsbewijzen, bankrekeningnummer, IBAN, bewijs van woonplaats...) via een website of per telefoon door aan iemand die beweert ons te vertegenwoordigen, zonder eerst de authenticiteit ervan te hebben gecontroleerd via onze officiële kanalen.
- Informeer naar het bedrijf waarvan uw gesprekspartner beweert deel uit te maken door de officiële contactgegevens (telefoonnummer, e-mailadres en postadres) via andere bronnen op te zoeken om de juistheid van de verstrekte informatie te controleren. Aarzel niet om

de identiteit van uw gesprekspartners te controleren door een e-mail te sturen of te bellen naar de telefoonnummers die op de officiële websites staan vermeld.

- Als een bericht afkomstig lijkt te zijn van een onbekende of twijfelachtige bron, klik dan niet op de links, open geen bijlagen en reageer niet op het bericht.

Voor meer aanbevelingen verwijzen wij u naar de educatieve informatie die online is geplaatst door de Autorité des Marchés Financiers in Frankrijk of door uw lokale toezichthouder.

➤ **Wat moet u doen als u denkt dat u het slachtoffer bent geworden van fraude?**

1. Als deze fraude verband houdt met Comgest, kunt u ons hiervan rechtstreeks op de hoogte stellen via info@comgest.com.
2. In geval van identiteitsfraude via WhatsApp meldt u het bericht, de groep en/of het verdachte profiel als volgt en verwijdt u het bericht van uw apparaat nadat u het hebt gemeld:
 - Een profiel melden: klik op het contact dat u wilt melden en klik vervolgens onderaan de pagina op 'Melden + telefoonnummer'.
 - Een groep melden: klik op de naam van de groep bovenaan de gesprekken en klik vervolgens onderaan de pagina op 'Groep melden'.
3. Als u de Franse nationaliteit hebt, doe dan een melding via Pharos (het officiële portaal van het ministerie van Binnenlandse Zaken voor het melden van illegale inhoud op internet): <https://internet-signalement.gouv.fr/>.