

IMPORTANT NOTICE: ATTEMPTS AT FRAUD THROUGH IDENTITY THEFT

Like many companies, we have noticed an increase in fraud attempts that misuse our company's name, visual identity or contact details, in particular through the creation of fake domain names designed to mislead the recipient, and, in some cases, those of former employees on instant messaging applications.

These attempts are designed to mislead investors by offering them fake financial products and investment opportunities, or by attempting to obtain personal or banking information.

We recommend that you remain vigilant to protect yourself and remind you that:

- Our official website is <https://www.comgest.com>.
- Comgest does not use social media or instant messaging applications (such as WhatsApp) as a means of contact.

➤ **Fraud and identity theft**

Fraud refers to an intentional act of deception or concealment aimed at obtaining an undue advantage to the detriment of others. It covers a wide range of unfair practices, such as identity theft when used for malicious purposes.

Identity theft involves knowingly appropriating the identity of a natural or legal person, or using their identifying details (name, logo, email address, official documents) with the aim of deceiving a third party. When it is used to obtain an unfair advantage or cause harm, identity theft constitutes a form of fraud and may also be considered a scam.

➤ **What steps should you take to protect yourself from fraud?**

- Be extremely vigilant about any unsolicited contact by telephone, email, text message, social media or instant messaging apps. Whatever the form (telephone, post, email or message), impersonation is common, widespread and easy to carry out.
- Do not disclose any personal information (telephone number, email address, identity documents, bank details, IBAN, proof of address, etc.) via a website or by telephone to anyone claiming to represent us without first verifying their authenticity through our official channels.
- Find out about the company your contact claims to represent by searching for its official contact details (telephone number, email address and postal address) through other sources in order to verify the accuracy of the information provided. Do not hesitate to verify the identity of your contacts by sending an email or calling the telephone numbers listed on the official websites.

- If a message appears to come from an unknown or dubious source, do not click on any links or open any attachments, and do not reply to it.

For further recommendations, please consult the educational information published online by the French Financial Markets Authority (Autorité des Marchés Financiers) or your local regulator.

➤ **What should you do if you think you have been a victim of fraud?**

1. If the fraud is related to Comgest, please notify us directly at info@comgest.com.
2. In the event of identity theft via WhatsApp, report the message, group and/or suspicious profile as follows, then delete the message from your device after reporting it:
 - Reporting a profile: click on the contact you wish to report, then click on "Report + phone number" at the bottom of the page.
 - Reporting a group: click on the group name at the top of the chats, then at the bottom of the page, click on "Report group".
3. If you are a French citizen, file a report with Pharos (the official portal of the Ministry of the Interior for reporting illegal content on the Internet): <https://internet-signalement.gouv.fr/>.