Cloned firm: The FSMA warns the public against theft of OGESIP Invest's identity

30/06/2026 Warning

The Financial Services and Markets Authority (FSMA) warns the public against an entity that is unlawfully active within Belgium.

Fraudsters are passing themselves off as OGESIP Invest, an institutional Sicav/Bevek (open-ended investment company) governed by Belgian law held by OGEO Fund. OGEO Fund is a Belgian institution for occupational retirement provision authorized by the FSMA.

OGESIP Invest does not have a website. However, persons usurping the identity of OGESIP Invest have set up a fraudulent website: https://www.ogesip-investment.com/. This website uses the information and contact details of OGESIP Invest without authorization.

The above website is **not authorized** to provide investment services in Belgium.

This is a '**Cloned firm**'. This is a form of fraud in which swindlers steal the identity of an authorized company in order to give consumers the impression that they are authorized to offer them regulated investment products or services, whereas this is not the case.

The FSMA thus **strongly advises against responding to any offers of financial service made by these persons** and **against transferring money** to any bank account number they might mention.

In order to prevent consumers from falling victim to this type of investment fraud, the FSMA makes the following recommendations:

Always check the identity of your interlocutor (have you checked its name, registered office, home country, contact details and whether it holds an authorization to make this type of offer?).
If you cannot clearly identify your interlocutor, it should not be trusted. If the company is based outside the European Union, you should be aware of the difficulty of legal recourse in the event of a dispute.

Check that the contact details for that company listed on the FSMA's website are the same as those found on the company's website.
Beware! Fraudsters frequently also steal the postal address of the authorized institution. Therefore, the fact that the correct postal address is used by your interlocutor is therefore not enough to confirm his/her/its identity!

Use online search engines to ensure that there is no other website under the name of the authorized company in question.
Beware! Fraudsters frequently use a web address that is very close to that of the official site of the company whose identity they have stolen, for example by adding a hyphen to the address, using a different extension (.com instead of .be, for example. etc.).

Compare the official information with the facts.
For example, if the person contacting you claims to represent a company based in Belgium but is contacting you from a foreign phone number, this should serve as a warning sign. Similarly, you should be wary if the company's website is in French or Dutch only, whereas the company claims to be based in a country with a different official language.

Use the online tools available that allow you to verify the date when the website used by your contact person.
If the website is very recent, this is a significant indication that it may not be trustworthy.

Lastly, be wary of (promises of) completely disproportionate gains.
Where a return seems too good to be true, it usually is.