



During recent months, the FSMA has observed a significant number of cases of investment fraud that take the form of stealing the identity of authorized companies ('cloned firms'). In this form of fraud, swindlers take on the identity of an authorized company in order to give consumers the impression that they have the authorization to offer them investment services, whereas this is not the case. The services they offer are entirely fraudulent. The FSMA therefore warns consumers.

### How do the fraudsters proceed?

In order to convince you to take them upon their offer of investments, the fraudsters lead you to believe that they are acting on behalf of firms that have the necessary authorization to offer such services and that are registered with the FSMA or another authority.

To this end, they usurp the names and other legal information of regulated providers and refer consumers, for example, to the official website of the FSMA to try to convince them that they are indeed authorized firms. Consumers are thus deceived, thinking they are dealing with a regulated entity, whereas the latter's identity has simply been stolen.

In some cases, the fraudsters also refer to the website of the *Autorité de contrôle prudentiel et de résolution* (ACPR), the French authority, and in particular to the register of financial agents (REGAFI) published on the latter site.

Consumers report:

*'The first thing they say when you contact them from Belgium is to type the company's name into your search engine.'*

*'To gain my trust and prove their good faith, [the contact person] invited me to go to the French website managed by the Banque de France which comprises a register of financial firms operating on French territory ([www.regafi.fr](http://www.regafi.fr)). After I had searched that site, I found the following link: ... Convinced of their good faith, I opened an account on their site.'*

*'Their contact person, a 'customer relations manager', pointed me to the REGAFI site to show me that the firm was registered under no. XXX. My question is: does that registration have any value?'*

### In what context may one come across such practices?

These types of identity theft may occur in any kind of investment fraud.

However, the FSMA invites you to be particularly wary of fraud involving cryptocurrencies, where this practice

seems extremely widespread.

The FSMA recently issued a warning against a significant number of such platforms that offer 'miracle' investments in cryptocurrencies that appear very simple and lucrative, but that are in fact scams (see our most recent [press release](#) dated 26 October 2018). It seems that a substantial number of these websites have stolen the identity of companies authorized to offer financial services in Belgium, referring to their authorization on the website of the FSMA (see the register of financial firms by the ACPR – REGAFI).

## How to avoid the trap?

This fraudulent practice may be difficult to detect and avoid. We therefore encourage you to take the following steps to ensure that your interlocutor is indeed who he or she claims to be:

- Verify the contact details for that company listed on the FSMA's website and check that they are the same as the one which the firm provides on its own site.

**Beware!** It is frequently the case that fraudsters also steal the postal address of the authorized company. The fact that the correct postal address is used by your interlocutor is therefore not enough to confirm their identity!

- Use online search engines to ensure that there is no **other website under the name of the authorized company in question**.

**Beware!** Swindlers often use a web address that is very close to that of the official site of the company whose identity they have stolen (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 your interlocutor claims to represent a firm based on 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 your interlocutor's website was created. If the website is very recent, this is a significant indication that it may not be trustworthy.
- If you have any doubt whatsoever about the identity of your interlocutor, contact the FSMA's services using the [consumer contact form](#).

**Source URL:** <https://www.fsma.be/en/warnings/fsma-warns-against-identity-theft-authorized-companies>