



## Veel te mooi om waar te zijn

*Van valse Facebookadvertenties tot fraude met cryptomunten<sup>1</sup>*



**Johan Corthouts,**  
Medewerker  
FSMA



**Brigitte Leën,**  
Medewerker  
FSMA

### ABSTRACT

Every day we see a wide range of financial scams being promoted through social media. Consumers are attracted by high-yield investments. Criminals make them believe that they can earn a lot of money. They tell stories about huge profits. Consumers lose all the money they put in the hands of criminals. None of the money is ever invested.

The consequences of this kind of financial crime go well beyond the financial losses involved. Investment fraud can destroy not just the victim's savings but also their mental and physical well-being.

The FSMA alert consumers to the risks of scams. We publish tips on how to recognise fraudulent activities. When the offer is 'too good to be true', it is probably a scam.

---

<sup>1</sup> De FSMA gaat vertrouwelijk om met de gegevens van consumenten. De namen van de melders van fraude in dit artikel zijn fictief.

The FSMA regularly updates a warning list of companies who are not authorised in Belgium or are known for their fraudulent business. The FSMA conducts research on investment fraud and is working together with the police and judicial authorities on its prevention.

Spaarders en beleggers, kijk uit. Oplichters proberen u geld afhandig te maken met de verkoop van financiële producten met hoge rendementen. Ze maken vele slachtoffers. Denk niet: het zal mij niet overkomen. Niemand is immuun voor oplichting.

Wie actief is op Facebook heeft ze zeker gezien, de nepadvertenties om te beleggen in cryptomunten. Om geld te verdienen, is het voldoende om te investeren in bitcoins en andere digitale munten. Winst verzekerd, was de boodschap. Beleggers werden ertoe aangezet om snel te handelen, want de kansen om fortuin te maken kunnen keren. Goedgelovige beleggers trapten in de val en verloren centen.

Bekende figuren zoals ondernemer Marc Coucke, komiek Philippe Geubels, Rode Duivel Vincent Kompany en televisiemaker Gert Verhulst deelden mee in de klappen. Oplichters gebruikten hun naambekendheid om beleggers op het verkeerde been te zetten. Hun foto's en valse getuigenissen verschenen in nepadvertenties op Facebook. "Ik verdien tienduizenden euro's per dag. Het is op dit moment letterlijk de snelste manier om geld te verdienen," zei Coucke zozegd in een geloofwaardig uitzend nieuwsbericht. Coucke en de andere bekende Belgen zijn medeslachtoffer van zulke nepadvertenties, die het sociale netwerk teisteren.



### **Belofte van torenhoge winsten**

Ook zonder de hulp van bekende Belgen slagen oplichters erin om beleggers om de tuin te leiden. Een belofte van torenhoge winsten volstaat. De lokroep van het geld trekt beleggers aan. Vaak verliezen ze hoge sommen geld. Dat overkwam André. Eind juli 2019 werd hij telefonisch gecontacteerd door Global Markets, een vals beleggingsplatform. André had nog nooit een belegging gedaan en kwam in de verleiding om daarmee te beginnen en zo hoge winsten te realiseren.

Hij startte zijn belegging met een bescheiden bedrag van 250 euro. Vervolgens stortte hij 5.000 euro op zijn *trading account*. “Na drie weken had ik 9.000 euro gemaakt. En ze zeiden dat als ik 12.000 euro toevoeg, ik een beter *account* krijg en een *swap free account* van 6 maanden. Wat ik dus gedaan heb... en 12.000 euro toegevoegd. Na zes weken stond mijn account op 50.000 euro,” schrijft André in een melding aan de FSMA.

En toen begon de miserie voor André. Zijn contactpersonen bij Global Markets hielden hem voor dat er problemen waren op de goudmarkt. Om zijn investering te redden, moest hij snel geld storten. Hij besloot 21.000 euro bij te storten, waardoor zijn totale investering 38.000 euro bedroeg.

“Mijn accountmanager bij Global Markets had mijn vertrouwen gewonnen en ik geloofde hem blindelings,” getuigt André. Dat vertrouwen ging heel ver. De oplichters namen van op afstand André’s computer over en schreven zijn geld over naar hun rekening.

De oplichters maakten schaamteloos misbruik van zijn vertrouwen en zetten hem almaar meer onder druk om in te stemmen met nog meer overschrijvingen. Intussen weet André beter. Zijn bankier gaf hem de raad geen nieuwe overschrijvingen te doen en klacht neer te leggen. André is ten einde raad. “Ik vrees dat ik mijn geld kwijt ben. ‘s Nachts slaap ik er niet meer van. *Please help me!*”

### Misbruik van vertrouwen

Niet alleen Facebook is een populair kanaal voor oplichters om slachtoffers aan de haak te slaan. Oplichters gebruiken ook andere sociale media om hun slag te slaan. Instagram bijvoorbeeld. Alexander raakte via die weg aan de praat met ene Stephanie Hampton. Deze dame doet uitschijnen dat ze een fantastisch leven leidt. Zonder geldzorgen. Haar profiel staat vol mooie foto’s. Ze doet aan *trading* met bitcoin en helpt graag andere mensen om ook op die manier succes te hebben. Maar deze Stephanie is in realiteit een ronselaar die werkt voor cryptofraudeurs.



Alexander heeft gedurende enkele maanden regelmatig contact met Stephanie via Instagram. Aanvankelijk twijfelt hij aan de oprechtheid van Stephanie, maar gaandeweg laat hij zich overtuigen. Stephanie weet hoe ze het vertrouwen van potentiële slachtoffers kan winnen en hen in de val kan lokken. Ze is geduldig. Ze is niet opdringerig. Ze is altijd beleefd. “Na acht maanden van praten, neem ik aan dat ik u kan vertrouwen,” liet Alexander haar weten.

Alexander koopt voor 750 euro bitcoins. Die stort hij door naar Spring Options, een ‘beleggingsplatform’ dat Stephanie hem aanraadt. De waarde van een bitcoin neemt op het ogenblik van de aankoop toe. Die evolutie is voor Alexander een teken van vertrouwen.



Wat daarna gebeurt, tart elke verbeelding. “Ik zie mijn kapitaal groeien. Eerst op rationele wijze. Vervolgens 2 à 3 dagen later, op irrationale wijze. In mijn enthousiasme sluit ik mijn ogen en zeg dat dit allemaal mogelijk is,” schrijft Alexander in een melding aan de FSMA. Alexander volgt via de website van Spring Option de evolutie van zijn investering op de voet. Na zeven dagen bedroeg zijn winst bijna 18.000 dollar. Wanneer hij besluit om het geld op te strijken, wordt hem gevraagd om meer geld bij te storten. Een bijkomende storting van 500 euro kan binnen de week uitgroeien tot een bedrag van 16.000 dollar. Alexander ruikt onraad en beslist om niet in te gaan op de vraag om bij te storten. Stephanie maakt zich kwaad en zegt dat hij moeilijk doet. Ze verbreekt alle contact. Alexander is zijn 750 euro kwijt.

De voorbeelden van André en Alexander illustreren hoe oplichters te werk gaan. De oplichters vragen beleggers om eerst een beperkt bedrag te storten. Daarna volgen snelle, gemakkelijke en hoge winsten. De beleggers kunnen deze informatie in real time volgen op een website. Maar alles wat getoond wordt, is nep. De oplichters bouwen een vertrouwensband op met hun slachtoffers. Daarna krijgen de beleggers de vraag om veel hogere bedragen in te leggen. Op die manier komen ze zagezegd in een ‘beter beleggersprofiel’ terecht en kunnen ze nog hogere winsten maken. Om hun boodschap kracht bij te zetten, maken de oplichters gebruik van agressieve marketingtechnieken. Van zodra beleggers niet bereid zijn om bijkomende centen te storten of wanneer ze hun geld terugvragen, wordt alle contact verbroken. Het geld is verloren. Beleggingen zijn er nooit mee gedaan. Het geld wordt onmiddellijk doorgesluisd naar andere rekeningen.

### **Fraudeurs hebben professionele organisatie**

Fraudeurs doen er alles aan om beleggers te doen geloven dat ze betrouwbaar zijn en dat ze de ideale partij zijn voor een investering. Daarom doen ze hun uiterste best om over te komen als een echte beleggingsonderneming. Wat hebben ze daarvoor nodig? Een eigen vennootschap. Een goed verzorgde en professioneel ogende website, inclusief beleggingsplatform. Een callcenter dat beleggers via mail, sociale media of telefoon te woord staat. Een reeks stromannen die reclame kunnen maken voor hun activiteiten. En een netwerk dat betalingen snel kan doorsluizen naar onbekende oorden of kan witwassen.

De oplichters komen nooit in beeld. Ze mijden elk fysiek contact met hun slachtoffers. Ze behoren tot een professioneel netwerk, dat georganiseerd is zoals een echt bedrijf met een ceo, een *head of sales* en trainers voor het callcenter. Ze doen beroep op reguliere bedrijven zoals webdesigners en hebben gewone werknemers in dienst in hun callcenters. Een goede organisatie is essentieel. Beleggingsfraude is *big business*. Sommige circuits die de FSMA onderzocht, zetten op enkele maanden tijd 50 miljoen euro om.

De FSMA doet onderzoek naar verschillende soorten van beleggingsfraude. Van zodra er een link met een financieel product of een financiële dienst is, is de FSMA bevoegd om



tegen fraude op te treden. Het gaat over piramide- en ponzsystemen op basis van een financieel product of financiële dienst; over oplichting bij de verkoop van binaire opties en forexproducten en over fraude met *boiler rooms* en *recovery rooms*. Momenteel is fraude met bitcoins of andere cryptomunten zeer populair (zie kader).

### *Schrijnende verhalen en schaamte*

De FSMA ontvangt dagelijks klachten over oplichting. Sommige beleggers verliezen enkele honderden euro. Anderen verspelen een half miljoen euro of meer. Sommigen zien het spaargeld van een heel leven in rook opgaan. Anderen verkopen hun huis om snel rijk te worden. De FSMA ontvangt ter zake schrijnende verhalen van consumenten. Het is slechts een tip van de ijsberg. De meeste slachtoffers van oplichterij schamen zich en blijven met hun verhaal zitten.

Mensen denken dat ze immuun zijn voor oplichting. Maar dat is een verkeerde inschatting. Iedereen kan slachtoffer zijn. Jong en oud. Arm en rijk. Hoog- en laaggeschoold. Bedrijfsleiders zijn een specifiek doelwit bij *boiler room*-fraude waarbij ze ongevraagd gebeld worden met mooie beleggingsvoorstellen. Gepensioneerden die net hun groepsverzekering ontvingen, vormen een aparte doelgroep. Oplichters gaan op zoek naar zogeheten *sucker lists* van mensen die interesse hebben voor beleggen. Iedereen die op zoek is naar net dat ietsje meer rendement dan op een spaarboekje is een potentieel slachtoffer van fraude.

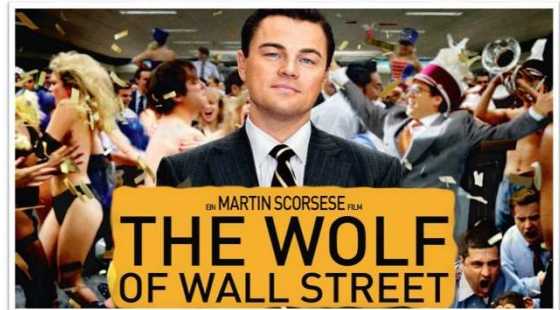
De FSMA ontving vorig jaar meer dan 2.000 meldingen van consumenten. Meer dan de helft daarvan gaat over fraude en onregelmatige aanbiedingen. Consumenten verliezen jaarlijks miljoenen euro. De FSMA **onderzoekt** onder meer op basis van deze meldingen het illegale aanbod van financiële diensten en producten in België. Ze deelt deze informatie met justitie zodat die kan optreden tegen fraudeurs. Deze samenwerking heeft onder meer geleid tot het blokkeren van frauduleuze websites (zie kader).

### *Preventie voorkomt fraude*

De kans is evenwel klein dat beleggers die fraudeurs geld hebben toegestoken die centen terugzien. Fraudeurs slagen erin om uit de greep van speurders te blijven. Vandaar het belang van preventie (zie kader). De FSMA publiceert op geregelde tijdstippen waarschuwingen over valse beleggingsplatforms en andere onregelmatige aanbiedingen. Op die manier helpt ze voorkomen dat beleggers in de val trappen en centen verliezen. Beleggers moeten zelf ook uitkijken voor fraude. Ga steeds na wie uw aanbieder is en verzamel alle mogelijke informatie over hem. Pas op voor beloftes over hoge rendementen. Als het te mooi is om waar te zijn, dan is het dat ook. Dat is onze belangrijkste boodschap.

Wie twijfelt aan die boodschap kijkt best naar de film *The Wolf of Wall Street*. Deze Amerikaanse prent van Martin Scorsese is gebaseerd op een waar gebeurd verhaal. Het hoofpersonage Jordan Belfort – vertolkt door Leonardo DiCaprio – verdient bergen geld met het oplichten van goedgegelovige mensen. Zijn beleggingsfirma Stratton Oakmont is gespecialiseerd in de verkoop van waardeloze aandelen. Die worden tegen hoge commissies verkocht. De geldmachine gaat pas echt aan het draaien wanneer de firma ook koersen van aandelen kunstmatig opdrijft en Stratton Oakmont hiervoor vette koerswinsten op zak steekt. De zaak stort in elkaar wanneer de FBI weet krijgt van de oplichtingspraktijken en Belfort bereid is om mee te werken aan het onderzoek in ruil voor strafvermindering.

De film is een voorbeeld van hoe een *boiler room* werkt. Stratton Oakmont schrok niet terug voor agressieve verkooptechnieken waarbij consumenten zwaar onder druk werden gezet. Deze manier van werken leverde Belfort&co de bijnaam *The Wolf of Wall Street* op. Belfort is momenteel actief als *motivational speaker*. Het goed kunnen uitleggen, is een belangrijk kenmerk van fraudeurs. Kijk uit en laat u niks aanpraten.



#### *Tips om beleggingsfraude te voorkomen*

- Wees op uw hoede voor beloften van buitensporige winst. Als een rendement te mooi lijkt om waar te zijn, is het dat ook.
- Controleer de identiteit van aanbieders van beleggingen. Vertrouw nooit een vennootschap die u niet duidelijk kan identificeren.
- Kijk uit voor vennootschappen die beweren een vergunning te bezitten. Vaak hebben ze die gestolen van andere vennootschappen.
- Check websites. Een website van recente makelij kan een aanwijzing van beleggingsfraude zijn.
- Pas op als u gevraagd wordt om geld over te schrijven naar een bankrekening in een land dat geen enkele band heeft met het land waar u woont of het land van herkomst van de vennootschap.
- Negeer telefoontjes van onbekende aanbieders.
- Bij twijfel contacteer de FSMA.
- In geval van fraude: dien klacht in bij de lokale politie en meld de fraude aan de FSMA.
- Laat u geen tweede maal vangen. Fraudeur beloven verloren geld terug te betalen na een nieuwe storting. Dat is een beproefde techniek om slachtoffers opnieuw geld te ontfutselen.





### *Wat doet de FSMA?*

- Vragen van consumenten over de betrouwbaarheid van aanbieders van beleggingsvoorstellen beantwoorden.
- Klachten van slachtoffers van frauduleuze beleggingsvoorstellen behandelen.
- Onderzoek naar informatie over onregelmatige aanbiedingen van financiële producten of diensten.
- Onderzoek naar bankrekeningen die gebruikt worden bij frauduleuze aanbiedingen.
- Publicatie van meerdere algemene waarschuwingen over *boiler rooms*, binaire opties en forex, alternatieve beleggingen, cryptofraude, ponzi- en piramidefraude en kredietfraude. In deze algemene waarschuwingen geeft de FSMA ook tips aan de consumenten.
- Publicatie van specifieke waarschuwingen met betrekking tot aanbieders van financiële producten en diensten.
- Publicatie van de waarschuwingen van buitenlandse toezichhouders via ESMA en IOSCO.
- Publicatie van een lijst van vennootschappen die op onregelmatige wijze actief zijn op het Belgisch grondgebied.
- Dossiers overmaken aan het Parket en in bepaalde dossiers samenwerken met de politie.
- Dossiers melden aan de Cel voor Financiële Informatieverwerking.
- Ondersteunen van het Meldpunt van de FOD Economie voor wat betreft frauduleuze aanbiedingen van beleggingen.
- Verspreiding van informatie over fraude aan consumenten op haar website en de website van Wikifin.

### *Kleine lexicon van beleggingsfraude*

Een **binaire optie** is een alles-of-niets-contract. Beleggers gokken erop dat de prijs van bijvoorbeeld een vat ruwe olie op een vooraf bepaald tijdstip boven of onder een bepaalde grens zit. Afhankelijk van hoe hij gokt, wint de belegger of verliest zijn volledige inzet. Er gebeurt veel fraude met de verkoop van zulke derivaten.

Bij **forex** kan de belegger speculeren op wisselkoersverschillen. Forex staat voor *foreign exchange*. Ook deze vorm van beleggen is bijzonder fraudegevoelig.

Een **boiler room** verkoopt waardeloze of onbestaande effecten tegen een veel te hoge prijs. Oplichters bellen potentiële slachtoffers ongevraagd op. Ze schrikken er niet voor terug om potentiële slachtoffers zwaar onder druk te zetten om in te gaan op hun aanbod, vandaar de naam *boiler room*.

Een **recovery room** benadert slachtoffers van oplichting met de belofte dat ze het geld dat ze verloren hebben, kunnen recupereren. Voor die 'dienstverlening' betalen ze een fiks bedrag. Dat geld verdwijnt in de zakken van oplichters.

**Fraude met cryptomunten** is een populaire vorm van fraude. Beleggers denken dat ze centen investeren in virtuele munten, maar hun geld belandt rechtstreeks op rekeningen van oplichters.

Bij **piramide- en ponzifraude** worden de winsten van beleggers uitbetaald met het geld van nieuwe beleggers. Deze vorm van fraude draait zo lang oplichters erin slagen om nieuwe beleggers aan te trekken.

Bij **kredietfraude** worden slachtoffers gevraagd om een reeks betalingen te doen voorafgaand aan de kredietverlening. Van zodra oplichters het geld opstrijken, verdwijnen ze met de noorderzon.

Beleggingsproducten die gelieerd zijn aan de verkoop van **wijn** en **diamanten** zijn de voorbije jaren in opmars. Ook deze aanbiedingen zijn vaak instrumenten van oplichting.