FSMA
AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN

Persbericht

DE FSMA WAARSCHUWT OPNIEUW VOOR 'RECOVERY ROOM-FRAUDE'

De FSMA waarschuwt opnieuw voor bepaalde ondernemingen die ervan verdacht worden *recovery room*-fraude te plegen.

Recovery room-fraude is de praktijk waarbij oplichters **slachtoffers van beleggingsfraude** voorstellen om hen te helpen hun verliezen goed te maken of **verloren tegoeden te recupereren**.

Doorgaans worden de slachtoffers ongevraagd gecontacteerd via telefoon of e-mail. De FSMA merkt echter ook dat slachtoffers via eigen opzoekingen op internet of via sociale media in contact komen met zogenaamde *recovery rooms*. Oplichters en hun ondernemingen stellen zichzelf voor als advocatenkantoren, boekhouders, maar ook als politiediensten of financiële toezichthouders. De oplichters deinzen er bovendien niet voor terug om de identiteitsgegevens van bestaande ondernemingen of officiële instanties te misbruiken om betrouwbaar over te komen.

De fraudeurs vragen voor hun dienstverlening een **vergoeding**. Slachtoffers van beleggingsfraude moeten deze **bijdrage vooraf betalen**. Dit is een duidelijke aanwijzing dat het om een *recovery room* gaat. Deze bijdrage dient bijvoorbeeld betaald te worden om bepaalde administratieve of juridische kosten te dekken of om belastingen te betalen. Dit zijn echter louter **fictieve kosten**.

In andere gevallen beweren de fraudeurs dat ze hun diensten **gratis** aanbieden. Het slachtoffer moet dan enkel toegang geven tot zijn computer (bv. via Anydesk). Op die manier krijgen de fraudeurs de mogelijkheid om spyware te installeren of toegang te krijgen tot de PC-Banking van de consumenten.

Het komt ook voor dat fraudeurs hun slachtoffers vragen om een wallet op een cryptoplatform te creëren en activeren.

In alle gevallen slagen de fraudeurs erin geld van de consument te ontfutselen. Eens de fraudeurs het geld hebben ontvangen, verdwijnen zij met de noorderzon en is het nagenoeg onmogelijk om de vergoedingen te recupereren. **De FSMA raadt dan ook absoluut af om in te gaan op dit soort aanbiedingen.**

De ondernemingen die op onregelmatige wijze actief zijn en waarvoor de FSMA het publiek waarschuwt, zijn de volgende:

- **Block Analysis,** https://blockanalysis.eu
- **Bridgehold,** www.bridgehold.co
- **Clear Path Reclaim,** https://clearpathreclaim.com
- **CoinStats (Cloned firm)**
- **Cryptex,** https://www.cryptex.to
- **Cryptomaia,** https://cryptomaia.com
- **Cyber Financial, Cyber Financial Recovery Ltd**, www.cyber.financial, www.cyberfinancial.llc,

- **Elite Advisory Group (Cloned firm),** https://eliteadvisory.consulting**;** https://eliteadvisory.ac, https://elite-advisory.group, https://eliteadvisory.group
- **Eudigitalassets, Eudigitalassetsoffice,** https://eudigitalassests.org
- **Financial Recovery Technologies,** https://financialrecoverytechnologies.org
- **Fraud Prevention and Investigations LTD**
- **Fusion FX,** https://fusionfx.online
- **Hunter Crypto,** https://huntercrypto.com
- **Reclaim Secure,** https://reclaimsecure.com
- **Sepa-Services,** https://sepa-services.net, https://sepa-services.pro
- **Stingray,** https://sting.gray.bz, https://stingray.ac, https//stng.click
- **Wellington Lawyers,** https://wellingtonlaywers.uk

De FSMA merkt op dat het aantal gevallen van identiteitsdiefstal nog steeds aan de orde van de dag zijn.

Onlangs stelde inderdaad de FSMA vast dat fraudeurs consumenten misleiden door zonder toelating de naam van een gekend bedrijf te gebruiken. De FSMA ontving namelijk meldingen over oplichters die zich voorstellen als:

- **Axa Recovery** (Cloned firm), via de websites « https://axarecovery.com, https://axarecovery.art »
- **BCB Group** (Cloned firm), via de website « https://bcb.app-ch.com »
- **CoinStats** (Cloned firm)
- **Elite Advisory Group** (Cloned firm), via de websites « https://eliteadvisory.consulting**;** https://eliteadvisory.ac, https://elite-advisory.group, https://eliteadvisory.group »
- **Getquin, QUIN Technologies GmbH** (Cloned firm), via de websites « www.getquin.com »
- **Guarda** (Cloned firm)
- **M2 Recovery Ltd** (Cloned firm), via de websites « https://m2recoveries.com, https://m2recovered.com »

Oplichters misbruiken ook de naam van **overheidsinstanties of toezichthouders** om zo betrouwbaar te lijken: ofwel doen ze zich voor als deze officiële instanties, ofwel beweren ze met deze instanties samen te werken.

***

Slachtoffers van beleggingsfraude krijgen vaak twee keer te maken met dezelfde oplichters: een eerste keer als plegers van beleggingsfraude en een tweede keer als plegers van *recovery room*-fraude. Het kan ook dat de plegers van de beleggingsfraude de gegevens van hun slachtoffers doorverkopen aan andere oplichters. **Iedereen die ooit het slachtoffer is geworden van beleggingsfraude moet zich ervan bewust zijn dat oplichters hun slachtoffers opnieuw kunnen viseren of hun gegevens kunnen doorverkopen.**

Hoe kan u *recovery room*-fraude herkennen en voorkomen?

- Indien u het slachtoffer bent geworden van beleggingsfraude, raden wij u aan steeds **klacht neer te leggen** bij de lokale politie.

- Wees uiterst voorzichtig wanneer u op **sociale media of internet** een reclameboodschap vindt waarin men voorstelt verloren bedragen voor u te recupereren.

- Indien u **ongewenst telefonisch gecontacteerd** wordt met een voorstel om de door u verloren bedragen te recupereren, vraag dan hoe die persoon te weten is gekomen dat u gelden verloren bent. Meldingen van fraude worden enkel gedeeld met gerechtelijke instanties en niet met private ondernemingen.

- Indien er u gevraagd wordt om **vooraf een bepaald bedrag te betalen, toegang te krijgen tot uw computer, of een wallet op een cryptoplatform te activeren**, ga hier dan niet op in en beëindig alle contact.

- **Financiële toezichthouders** zoals de FSMA zijn niet bevoegd om verloren gelden te recupereren en zullen dus ook niet met deze bedoeling contact opnemen met slachtoffers van beleggingsfraude.

Wilt u controleren of verrichtingen die u worden voorgesteld in overeenstemming zijn met de financiële regelgeving? Gebruik dan de zoekfunctie op de website van de FSMA. U kan de FSMA ook rechtstreeks contacteren via het contactformulier fraude.

Brussel, 26 november 2026

Perscontact Jim Lannoo
Woordvoerder/Adjunct-directeur
Communicatie en Financiële Educatie
T direct + 32 2 220 57 06
E-mail Press@fsma.be