

Gevolgen van de Covid-19 crisis op het witwassen van geld en de financiering van terrorisme.

De huidige crisis als gevolg van het uitbreken van de wereldwijde Covid-19 pandemie stelt onze samenleving voor ongekende uitdagingen. De nationale overheden hebben als belangrijkste prioriteit het onder controle krijgen van de situatie op medisch vlak, maar proberen daarnaast ook de omvang en de gevolgen van de economische crisis zoveel mogelijk te beperken. Hoewel de huidige situatie geen precedent kent, hebben kleinere crisissen in het verleden aangetoond dat criminelen onder het motto “never waste a good crisis” zeer snel kunnen inspelen op veranderende en extreme economische omstandigheden. Volgens rapporten van Europol¹, Interpol² en de FATF³ hebben criminele organisaties op internationaal vlak al gebruik gemaakt van de Coronacrisis om hun bestaande modi operandi aan te passen of om nieuwe criminele activiteiten te ontwikkelen.

Met deze nota wil de CFI de melders sensibiliseren voor de effecten op korte termijn van de huidige situatie op de criminaliteitsvormen onderliggend aan witwassen, die zich vooral situeren op het vlak van oplichting. Uit de studies van internationale organisaties en de analyse van de eigen dossiers heeft de CFI een aantal concrete typologieën geïdentificeerd die de melders mogelijk kunnen helpen om deze vormen van oplichting te detecteren en daarna via meldingen de huidige analyse bij te stellen.

De verschillende vormen van oplichting die vastgesteld werden hebben vooral betrekking op de verkoop van materiaal gebruikt voor de bestrijding van het Coronavirus en om de verspreiding van de ziekte COVID-19 tegen te gaan. Het gaat onder andere om beschermingsmateriaal zoals mondkapjes en (mogelijke) geneesmiddelen voor de ziekte. In het vervolg van de tekst wordt naar deze goederen verwezen als ‘COVID 19-materiaal’.

Deze nota herneemt een aantal werkwijzen en indicatoren. Op zich volstaat een indicator niet om automatisch te kunnen spreken van een vermoeden van witwassen. Het voorkomen van meerdere elementen die hierna beschreven worden zou echter wel aanleiding moeten geven tot een bijkomende controle van de verrichting.

Verder zou de CFI de melders willen vragen om een mogelijk verband met de Coronacrisis te signaleren door bij de reden van melding in het online-meldsysteem de term “COVID19” te vermelden.

¹ <https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic>

² <https://www.interpol.int/>

³ <https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html>

1. Oplichting gericht op bedrijven

a. Werkwijzen

Bij de oplichting gericht op bedrijven zijn er twee werkwijzen die regelmatig terugkomen:

- Het coronavirus wordt gebruikt als pretext om betalingen te onderscheppen
- De criminelen doen zich voor als producenten en verdelers van COVID 19-materiaal

Het coronavirus wordt gebruikt als pretext om betalingen te onderscheppen

Fenomenen als 'CEO-fraude' en 'Business Email Compromise-fraude' (BEC-fraude) zijn na het voeren van verschillende preventiecampagnes algemeen bekend binnen het bedrijfsleven. De criminelen maken echter gebruik van de lockdown en de precaire economische situatie van vele bedrijven als gevolg van de huidige crisissituatie om de bestaande detectiemechanismen te omzeilen.

Hierbij twee voorbeelden :

- Criminelen doen zich voor als zaakvoerder van een onderneming en contacteren in die hoedanigheid de financiële instelling van die onderneming. De zogezegde zaakvoerder verklaart dat hij net als zijn collega's van thuis uit werkt en dat hij door een gebrekkige organisatie binnen zijn bedrijf de normale veiligheidsprocedures met betrekking tot betalingen, zoals de dubbele handtekening, in de huidige situatie niet kan volgen. Hij dringt hierbij aan op het uitsluitend voeren van de communicatie via email.

- Door opnieuw een gebrekkige organisatie als gevolg van de huidige crisis als excuus te gebruiken kunnen criminelen aandringen op de betaling rechtstreeks op de rekeningen van de productiesites van een bedrijf, en niet op de centrale rekening zoals gebruikelijk. Hierbij kunnen problemen met de boekhouding of met de cashpositie van het bedrijf ingeroepen worden. Dit frauduleus scenario laat toe om geldstromen die kaderen in een bestaande zakelijke relatie af te leiden naar de rekeningen van de oplichters.

Ook op het vlak van cybersecurity vormt het uitgebreide thuiswerk in toenemende mate een risico. Criminelen kunnen via veiligheidslekken toegang krijgen tot vertrouwelijke documenten en deze informatie gebruiken om complexe fraudeschema's op te zetten. De diefstal van vertrouwelijke informatie lag immers ook in het verleden al aan de basis van het succes van CEO-fraude en BEC-fraude.

De criminelen doen zich voor als producenten en verdelers van COVID 19-materiaal.

Door gebruik te maken van 'social engineering' kunnen criminelen zich voordoen als verkopers van COVID 19-materiaal. De permanente staat van urgentie waarin zowel de overheid als de private spelers zich bevinden bij het aankopen van dergelijk materiaal maakt hen kwetsbaar voor fraude.

Om hun aanbod te onderbouwen kunnen criminelen:

- Valse documenten produceren
- Valse internetsites creëren
- Schermvennootschappen opzetten
- Zich uitgeven voor bestaande bedrijven met een goede reputatie binnen de sector

b. Indicatoren met betrekking tot de slachtoffers

- *'Nieuwe' rekening begunstigde*

De klant onderhoudt zakelijke relaties met een aantal mede-contractanten. Plots wil hij echter een overschrijving uitvoeren:

- ten gunste van een nieuwe begunstigde en/of
- naar een rekening in een land waar hij geen activiteit uitoefent.

De financiële instelling doet er goed aan om een verhoogde waakzaamheid aan de dag te leggen wanneer een betaling uitgevoerd wordt naar een nieuwe begunstigde die snel gevolgd wordt door een nieuwe betalingsopdracht. De fraudeurs proberen immers vaak snel na een eerste succes een tweede betalingsopdracht te geven.

- *Tegenstrijdigheden bij de nieuwe begunstigde*

Volgende signalen kunnen voorkomen bij de begunstigde van een transactie:

- De begunstigde is een schermvennootschap
- De begunstigde is een nieuwe speler op de markt en heeft geen gedocumenteerde ervaring in de handel in COVID 19-materiaal.
- De begunstigde is niet de producent van het materiaal, maar een derde die geen bewezen handelsrelatie heeft met de producent.
- De begunstigde heeft geen duidelijke eigen economische activiteit
- De rekening van de begunstigde bevindt zich in een land dat ogenschijnlijk geen verband houdt met de uit te voeren transactie.

- *Dringend karakter van de verrichting*

De klant dringt sterk aan op het dringend karakter van de uit te voeren verrichting. Deze houding kan het gevolg zijn van de druk die de oplichters uitvoeren op de klant. De criminelen dreigen dikwijls om de zeer gewilde goederen te verkopen aan een andere partij indien niet snel betaald wordt.

- *Frauduleuze domeinnamen*

De betalingsinstructies bij fraude kunnen afkomstig zijn van mailservers of emailadressen waarvan de naam licht afwijkt van de gebruikelijke naam van de klant, door een beperkt aantal karakters weg te laten of toe te voegen.

Bij meer gesofistikeerde vormen van oplichting wordt de mailserver van de klant gehackt en worden instructies voor betaling doorgegeven vanuit de gebruikelijke mailadressen.

- *Tegenstrijdigheden in de documentatie*

De stavingsstukken die aan de professionele handelaar worden overgemaakt kunnen tegenstrijdigheden vertonen. Zo kunnen de berichten die uitgewisseld werden tussen de klant en zijn zogezegde mede-contractant sporen van phishing vertonen. Daarnaast werd ook vastgesteld dat oplichters valse internetsites opzetten om een activiteit als verkoper van COVID 19-materiaal te simuleren. De algemene voorwaarden en het niveau van detail van de beschikbare informatie op dergelijke valse sites zijn meestal zeer beperkt.

c. Indicatoren met betrekking tot de daders

- *Abnormaal transactiebedrag*

Het bedrag dat ontvangen wordt op de rekening is incoherent met het profiel van de begunstigde. In het geval van 'money mules' gaat het om personen met een beperkt inkomen die plots een betaling van meerdere tienduizenden euro's op hun rekening ontvangen.

- *Inconsequenties in de economische activiteit van de klant*

De klant opent een rekening voor het ontvangen van een salaris die nadien gecrediteerd wordt door overschrijvingen uit het buitenland voor grote bedragen.

Voorbeeld:

Een klant is loontrekkende bij een Belgische bank en ontvangt éénmalig een betaling van een Franse onderneming met als mededeling « Paiement de la facture 123456 ».

De reden van de ontvangen betalingen stemt niet overeen met de economische activiteit van de klant als natuurlijke- of rechtspersoon.

Voorbeeld:

Een vennootschap opgericht met een zeer algemeen maatschappelijk doel ontvangt plots betalingen die verband houden met de verkoop van COVID 19-materiaal.

2. Oplichting gericht op particulieren

De gevallen van fraude gericht op particulieren hebben betrekking op oplichting en op de schending van het intellectueel eigendomsrecht. De criminele schema's zijn klassiek:

- COVID 19-materiaal wordt verkocht maar nooit geleverd.
- Nagemaakt materiaal wordt verkocht
- Verkoop van geneesmiddelen vindt plaats buiten de toegelaten verkoopkanalen

Deze vormen van oplichting en fraude spelen zich voor een groot deel online af. Naast het gebruik van online-handelsplatformen worden ook op grote schaal reclamemails verstuurd (SPAM) en wordt gebruik gemaakt van advertenties op sociale media. Meer details worden verstrekt in de analyses van Europol, Interpol en de FATF, waarnaar in voetnoot verwezen wordt.

Volgende elementen kunnen wijzen op mogelijke oplichting:

- *Indicatoren in verband met de aard van de goederen die verkocht worden*

Volgende begrippen kunnen verband houden met de frauduleuze verkoop van COVID 19-materiaal:

- COVID-19
- Coronavirus
- SARS-CoV-2
- Masker
- Mask
- FFP2
- FFP3
- "(personal) protective equipment" ou "PPE"
- Chloroquine - Hydroxychloroquine - Azithromycine
- Plaquenil
- Hand sanitizer
- Desinfectant

- Alcohol 70%
- Ethanol 70%
- Face shield
- Hazmat suits
- Decontamination suits
- Ventilator, respirator, or breathing machine
- Kunstmatige beademing
- Beademingsapparaat

- *Indicatoren in verband met de prijs van de goederen*

Abnormaal hoge of lage prijs in vergelijking met de courant gehanteerde prijzen.

- *Indicatoren in verband met de begunstigden van de transactie*

De begunstigde is een schermvennootschap of is niet actief in de handel van COVID 19-materiaal

- *Indicatoren in verband met het distributiekanaal*

De verkoop van de goederen gebeurt buiten het normale distributiekanaal
