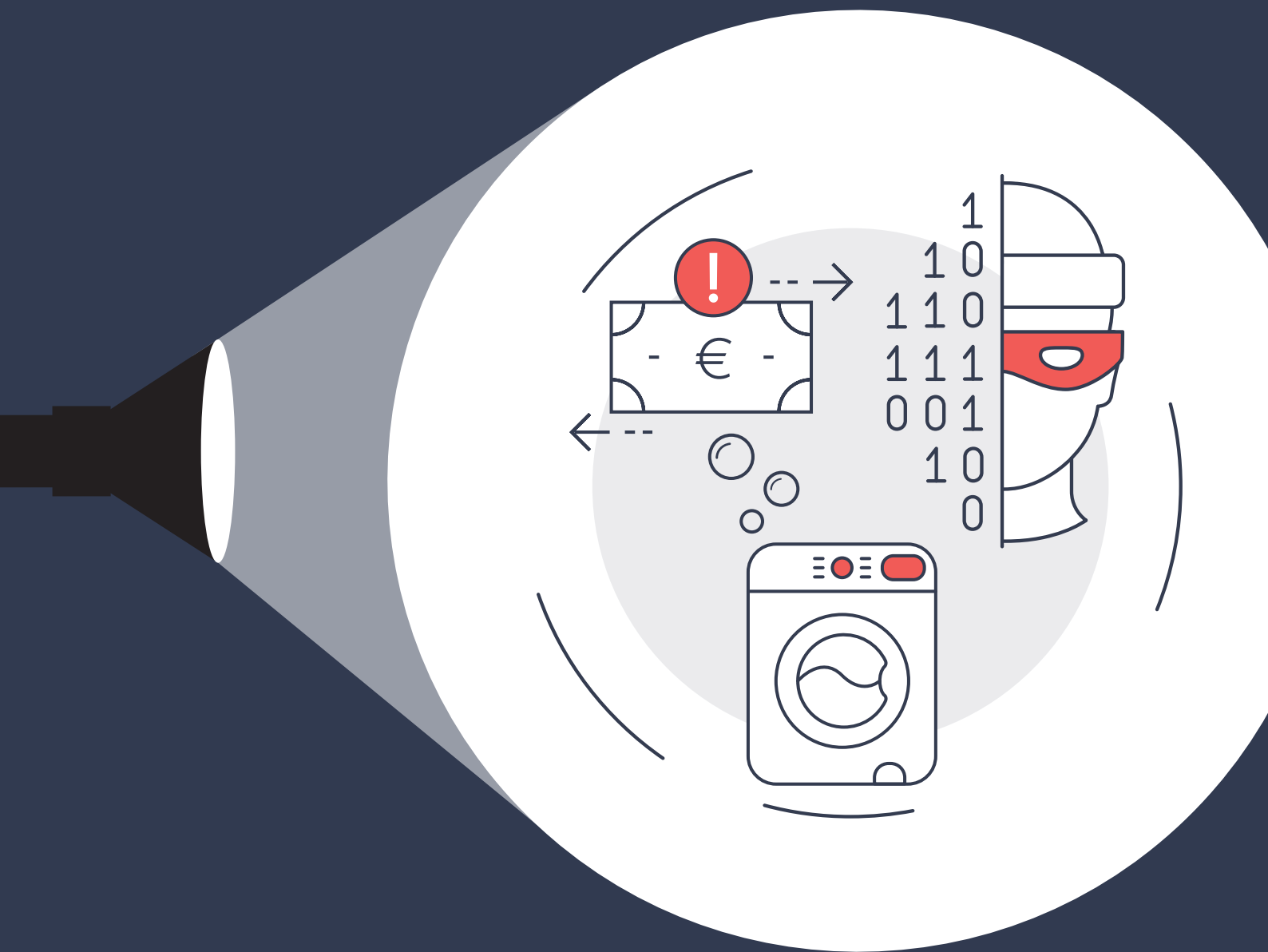


Banken: gatekeepers in de strijd tegen witwassen



Banken nemen hun verantwoordelijkheid in de opsporing van frauduleuze praktijken

Geld circuleert. Het doet de economie draaien. Banken vervullen daarbij een cruciale rol doordat ze financiële transacties en betalingen mogelijk maken. Maar er is ook een keerzijde aan geld: soms wordt het gebruikt om criminele activiteiten zoals terrorisme te financieren. Of wordt geld uit criminele milieus witgewassen door het keer op keer over te schrijven naar andere rekeningen. Na een tijdje lijkt crimineel geld zo helemaal proper of legaal te zijn.

De strijd tegen witwassen en terrorismefinanciering blijft uitdagend, en banken spelen vandaag een sleutelrol in het opsporen van financiële fraude.

Welke inspanningen banken leveren als gatekeeper in de strijd tegen witwassen en financiering van terrorisme, lees je in deze brochure.



NALEVEN EN OPVOLGEN VAN WETGEVINGEN

Banken zijn onderworpen aan de anti-witwaswetgeving en spelen een hoofdrol in de detectie van de financiële criminaliteit. De Belgische wetgeving is gestoeld op **Europese richtlijnen** (EU AMLD) en **internationale standaarden** (FATF/GAFI), die de **laatste jaren nog strenger** omkaderd werden (cfr. AML III, IV, V, VI, ...). Meer concreet betekent dit:

- Het toepassingsgebied werd uitgebreid en een meer instellingen moeten aan verplichtingen voldoen.
- Er werden nog hogere sancties vastgelegd (tot 10% van de jaaromzet van de instelling) voor het niet naleven van de regelgeving.
- Men koos voor een op risico's gebaseerde aanpak, geen "tick the box"-aanpak, maar individuele risicobeoordelingen (geen standaardisering mogelijk).
- Toezichthouders worden meer geïnspecteerd.
- Er is meer risico op imagoschade telkens er een schandaal opduikt.

De rol als **gatekeeper in de strijd tegen witwassen stopt niet bij het voorafgaand controleren van de identiteitskaart van de klant** maar vergt een **continue waakzaamheidsverplichting** doorheen de zakenrelatie met **tal van verplichtingen**:

- Know your customer "KYC"
- Know your transaction "KYT"
- Checken van de oorsprong van tegoeden
- Risk based approach
- Naleving van financiële embargo's
- Beperking op het gebruik van cash
- Meldingsplicht aan CFI (vermoedens van witwassen)
- Meldingsplicht aan Schatkist (embargo's)
- ...





Know your customer

De strijd tegen het witwassen van geld heeft een grote invloed op de **relatie tussen de bank en de klant**. Een klant die een rekening wil openen bij een bank, moet zich namelijk eerst identificeren. Dankzij de goede wil van de klant die ermee instemt zijn identiteit en andere gegevens mee te delen, kan de bank de klantrelatie correct inschatten en eventueel gepaste maatregelen nemen om financiële criminaliteit te bestrijden. Om uit te leggen hoe alles werkt, maakte Febelfin de brochure "**Waarom vraagt mijn bank mijn identiteitsgegevens?**" die banken kunnen gebruiken om hun klanten te informeren over waarom banken deze gegevens opvragen en waarvoor deze gegevens worden gebruikt.

De brochure gaat o.a. in op de informatie en documentatie die de bank moet verzamelen alvorens ze financiële diensten kan aanbieden. Meer precies betekent dit dat:

- er nood is aan identificatie en verificatie via bewijsstukken.
- Voor **natuurlijke personen** houdt dit in:
 - verificatie van gegevens (naam, voornaam, geboorteplaats, geboortedatum, ...) via inlezen elektronisch identiteitskaart (natuurlijke personen met Belgische nationaliteit) of paspoort (natuurlijke personen met andere nationaliteit);
 - onderzoeken of een persoon een 'specifieke risicoverhogende status' heeft (bv. Politically Exposed Persons, ...).
- Voor **rechtspersonen** is er specifieke informatie vereist, zoals o.a.:
 - geactualiseerde statuten;
 - duidelijkheid over de identiteit van de bestuurders, de Uiteindelijke Begunstigden (UBO's);
 - de bepalingen inzake bevoegdheid om rechtspersoon te verbinden;
 - optreden van lasthebbers (=volmachthouders, agenten) duidelijk in kaart brengen.

Dit proces moet periodiek worden overgedaan (= doorlopende waakzaamheid). Dat houdt in dat banken telkens opnieuw verschillende zaken moeten opvolgen:

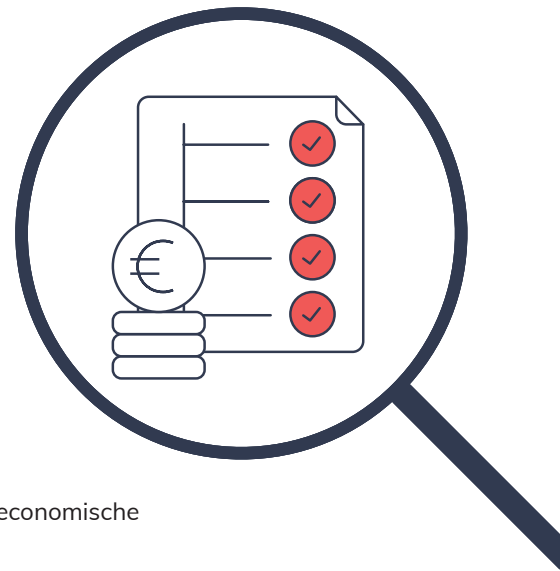
- Nieuw adres?
- Nieuwe statuten?
- Nieuwe UBO's? => Onderneming moet UBO's identificeren in het UBO-register en de bank hiervan verwittigen.
Meer info: **Wat je moet weten over het UBO-register | Febelfin**
- Bank herbegint de oefening om na te gaan of dit impact heeft op het risicoprofiel en maatregelen die ze moeten nemen.
- ...

Bovenstaande opsomming is niet volledig en onderworpen aan strikte wetgeving en aanbevelingen van de Nationale Bank van België.

Know your transaction

Banken moeten steeds nagaan of een verrichting strookt met de kenmerken van de cliënt en met het doel en de aard van de relatie. Zo moeten ze “atypische” verrichtingen gaan opsporen op grond van haar objectieve kenmerken of op grond van de kenmerken van de cliënt, zoals bijvoorbeeld:

- abnormaal complexe verrichtingen
- verrichtingen voor een ongewoon hoog bedrag
- intrinsiek ongebruikelijke verrichtingen zonder kennelijke economische grondslag of legitimiteit
- verrichtingen die niet lijken te stroken met het profiel van de cliënt



Risk Based approach (een op risico's gebaseerde aanpak)

Banken moeten hun AML-inspanningen en -middelen maximaal richten op het beperken van het risico om misbruikt te worden voor witwassen of voor de financiering van terrorisme. Deze risicogebaseerde benadering moet de financiële instellingen toelaten om minder verregaande maatregelen te kunnen treffen in situaties waar de risico's gering zijn en om de aldus vrijgekomen middelen aan te wenden voor het toepassen van verscherpte maatregelen ten aanzien van situaties waar de risico's groter zijn.

Als een bank vaststelt dat er bepaalde AML-risicoverhogende factoren zijn, dan moet ze:

- meer informatie inwinnen ter verificatie van informatie;
- verhoogde aandacht & controle uitvoeren op transacties;
- sneller gegevens actualiseren;
- en uiteraard: elk vermoeden van witwassen melden aan CFI en eventueel relatie stopzetten.

Banken moeten **conform de antiwitwaswet** op elk moment een volledig op risico's gebaseerde benadering kunnen toepassen. Dit betekent dat ze de **risico's op witwassen** die aan **iedere individuele klant** zijn verbonden moet kunnen **analyseren en mitigeren**. Om een idee te geven van de omvang: In 2019 ging het om de opvolging van zo'n **18.787.773 klanten**¹ waarvan 94,3% natuurlijke personen en 5,7% rechtspersonen zijn.

Melden van verdachte transacties

Dankzij bovenvermelde procedures kunnen banken hun **juridische rol** in de strijd tegen het witwassen van geld optimaal invullen en **verdachte transacties of verdachte feiten melden** aan de Cel voor Financiële Informatieverwerking (CFI). Zo kunnen deze grondiger worden doorgelicht en eventueel gesignaleerd worden aan het parket. Uit de cijfers van de CFI blijkt trouwens dat de **banken een van de voornaamste actoren** zijn in de strijd tegen het witwassen van geld.

In 2020 melden de kredietinstellingen 17.678 **verdachte transacties aan de CFI** en lagen ze aan de basis van **55%** (stijging van 12% t.o.v. 2019)² van de witwasdossiers die door de CFI doorgespeeld werden aan de gerechtelijke overheden. Het gaat hier over een bedrag van 1,9 miljard euro².

Om aan alle verplichtingen, inclusief de verplichting om verdachte transacties te melden aan de CFI, en wetgeving te voldoen vergt dit uiteraard verregaande investeringen in controle- en opsporingsprocedures, het versterken van interne organisaties (opleiden van personeel en bijkomende aanwervingen, ...), maar ook verregaande samenwerking tussen banken onderling en met andere organisaties en de overheid.



¹ Febelfin enquête afgenomen in 2020 waarbij de data betrekking hebben op de situatie per 31/12/2019 bij 18 banken waaronder de 4 grootbanken.

² Bron: Jaarverslag CFI 2020: [jv2020.pdf](#) (ctif-cfi.be)

INVESTEREN IN CONTROLE-EN OPSPORINGSPROCEDURES

De maatschappij beschermen tegen witwaspraktijken en terrorismefinanciering is een absolute prioriteit voor de Belgische banken. De voorbije jaren hebben banken verder geïnvesteerd in hun controle- en opsporingsprocedures:¹

- De Belgische banken hebben in 2019 voor meer dan 93 miljoen euro geïnvesteerd in hun compliance-AML departementen.
- Banken investeren ook massaal in tools om processen voor onboarding, screenings en de monitoring van transacties te automatiseren. Zo verloopt 95% van de periodieke 'name screenings' reeds automatisch.

VERSTERKEN VAN INTERNE ORGANISATIE

Daarnaast hebben ze hun interne organisatie versterkt om de strijd tegen witwaspraktijken verder op te voeren en hun verantwoordelijkheid als gatekeepers meer dan ooit op te nemen:

- In België houden zich naar schatting meer dan 1.600 bankmedewerkers dagdagelijks bezig met de strijd tegen het witwassen. Maar in de praktijk reikt dit veel verder, en heeft iedere bankmedewerker hier continue aandacht voor. Bovenstaande toont aan dat de strijd tegen witwassen niet alleen wordt opgevolgd door compliancediensten maar door alle diensten binnen de bank, in eerste instantie door medewerkers die in contact komen met de klant.
- 61% van de banken voorziet in 2021 bijkomende investeringen voor aanwerving van bijkomend personeel in het kader van de strijd tegen witwassen en de financiering van terrorisme.
- Bijna elke financiële instelling (94,4%) organiseert specifieke bijscholingen voor haar medewerkers in het kader van AML. Dit kan gaan van e-learning, tot klassieke opleidingen of zelfstudie. In 2019 hadden 44.000 bankmedewerkers (of 89% van alle bankmedewerkers in België) al minstens 1 keer een specifieke AML-opleiding gevolgd.

¹ Febelfin enquête afgenomen in 2020 waarbij de data betrekking hebben op de situatie per 31/12/2019 bij 18 banken waaronder de 4 grootbanken.

Banken cruciale schakel in een groter geheel

Het is duidelijk dat de banken een fundamentele schakel zijn om witwassen zoveel mogelijk tegen te gaan en op te sporen. Maar ze maken slechts een onderdeel uit van een groter geheel. De strijd tegen witwassen zou gebaat zijn met meer mogelijkheden rond informatie-uitwisseling, niet alleen tussen financiële instellingen onderling, maar ook met andere publieke instanties.

SAMENWERKING TUSSEN BANKEN

Banken wisselen onderling expertise en know-how inzake 'Know Your Customer' (KYC) utilities uit. Dat leidt tot verdere administratieve vereenvoudiging zowel voor de klant als voor de bank, maar versterkt ook de kwaliteit van de KYC-data en spoort banken aan om gebruik te maken van nieuwe technologieën (zoals bv. blockchain) om processen te automatiseren en te digitaliseren.

Febelfin volgt zo diverse projecten op om de KYC-diensten (know-your-customer) te optimaliseren, met name voor de identificatie van bedrijven en particulieren. Hiervoor ondersteunt Febelfin het bedrijf Isabel Group om het Kube-systeem te ontwikkelen, waarmee bedrijven zich kunnen identificeren via een systeem dat blockchaintechnologie gebruikt om de identiteit van gebruikers te verifiëren. Dankzij dit systeem kunnen klanten van financiële instellingen makkelijker, sneller en nauwkeuriger worden geïdentificeerd. Uit de enquête van Febelfin¹ bleek dat de meeste financiële instellingen zeer positief staan tegenover het gebruik van data sharing utilities (zoals o.a. Kube of Itsme).

Maar het is **banken niet in alle omstandigheden toegelaten om informatie over verdachte transacties of klanten te delen met andere banken**. Om dit mogelijk te maken is er een **juridisch kader nodig voor het veilig en wettelijk delen van data en gegevens**.

¹ Febelfin enquête afgenomen in 2020 waarbij de data betrekking hebben op de situatie per 31/12/2019 bij 18 banken waaronder de 4 grootbanken.

OVERLEG TUSSEN BANKEN EN OVERHEIDSINSTANTIES

In 2020 heeft Febelfin naar aanleiding van de 'FinCEN Files' nauwer overleg tussen de financiële sector en de openbare instanties (overheid, NBB, antiwitwascel, gerechtelijke autoriteiten, FSMA, enz.) aanbevolen om **efficiënt informatie uit te wisselen** en **gezamenlijk de strijd op te voeren tegen witwaspraktijken**.

Vandaag is het zo dat individuele **banken informatie bezorgen aan de overheid en de antiwitwascel**, maar daar stopt het vaak. Ze kunnen onderling maar heel beperkt informatie uitwisselen en krijgen beperkte feedback. Febelfin pleit dan ook voor **meer samenwerking tussen de financiële sector en de publieke instanties** (overheid, antiwitwascel, gerechtelijke instanties, etc.) om op een veilige manier informatie uit te wisselen, om zo de efficiëntie te verhogen en de handen in elkaar te slaan in de strijd tegen fraude en witwassen.

“Laat banken en overheden met elkaar via een veilige omgeving informatie uitwisselen over verdachte transacties zodat ze korter op de bal kunnen spelen en kunnen vermijden dat zwart geld wordt witgewassen.”

- Karel Baert

Dergelijke vormen van samenwerking tussen alle betrokken stakeholders werden reeds op poten gezet in andere **Europese landen**, zoals Nederland en het Verenigd Koninkrijk. Banken zijn absolute voorstander om ook in België een dergelijk platform op te richten.

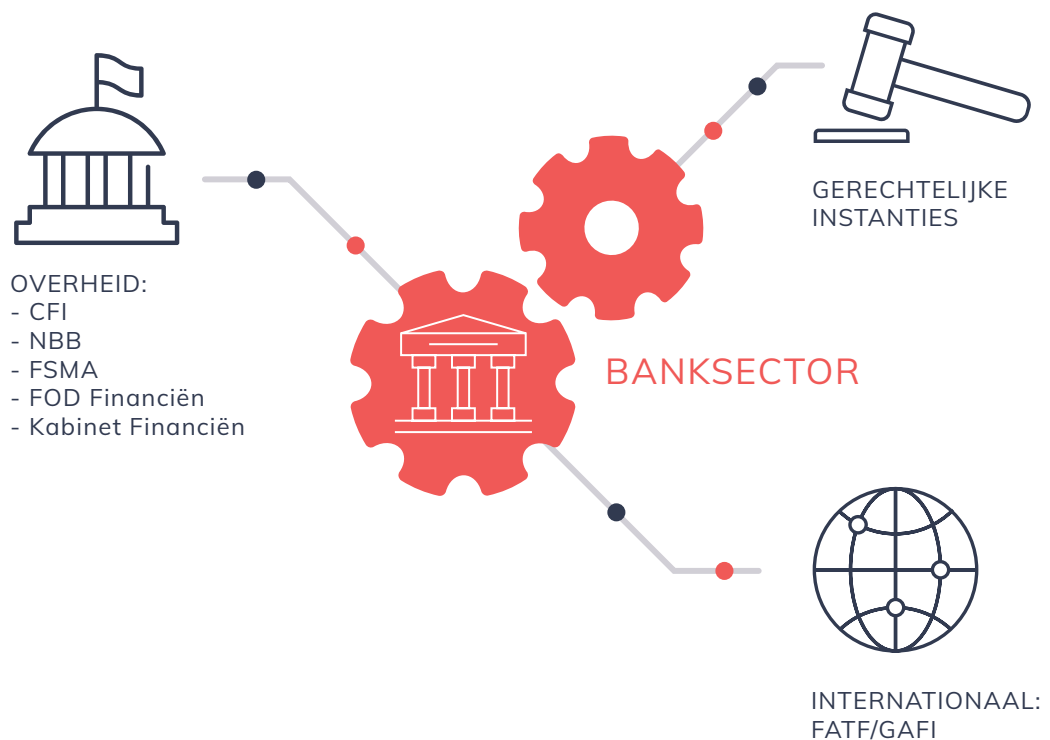
Dit pleidooi heeft nu gehoor gevonden bij de overheid en een dergelijke Privaat-Publieke Samenwerking wordt opgezet naar analogie met de voorbeelden uit de buurlanden. Een samenwerkingsprotocol werd opgemaakt om dit overlegplatform op te richten en vorm te geven. Partners in dit project zijn CFI, NBB, Kabinet Financiën, MinFin (Schatkist), Assuralia, FSMA en de banksector vertegenwoordigd door Febelfin. De doelstellingen van het platform zijn:

- het uitwisselen van informatie en expertise over vastgestelde AML-ontwikkelingen, trends, nieuwe risico's, mechanismen en typologieën;
- het bespreken van onderwerpen inzake AML/CFTP die voor de verschillende deelnemers relevant zijn;

- het voorstellen van richtlijnen en het verstrekken van feedback over de toepassing van de wettelijke AML/CFTP-verplichtingen, in het bijzonder over het detecteren en rapporteren van verdachte transacties;
- het opstellen van adviezen of voorstellen van initiatieven ter bevordering van de AML/CFTP aan de beleidsverantwoordelijken;
- het onderzoeken van de mogelijkheden om rekening houdend met de wettelijke bepalingen inzake beroepsgeheim en de verwerking van persoonsgegevens, al dan niet dossierspecifieke, data in het kader van AML/CFTP te delen en het desgevallend voorstellen van juridische en technologische oplossingen voor het uitwisselen van deze data via digitale weg.

Dit samenwerkingsverband zal ongetwijfeld bijdragen tot een **juridisch kader om data en gegevens veilig en wettelijk te delen**.

Stakeholders AML in België:



EUROPEES LUIK

De sector volgt ook nauwgezet de werkzaamheden van de **Europese Unie** ter zake. Europa buigt zich namelijk over een hervorming van de regels tot bestrijding van witwaspraktijken en wil een **single rulebook** uitwerken om de **regelgeving in de hele Unie te harmoniseren, bijvoorbeeld door te werken met rechtstreeks toepasbare verordeningen**. De harmonisering zal zorgen voor een meer **uniforme toepassing van de regels en zal de antiwitwaswetgeving efficiënter** maken. Daarnaast worden ook Europese wetsvoorstellen verwacht om te evolueren naar een Europese anti-witwas toezichthouder.

Samen met de Europese Banken Federatie (EBF) heeft Febelfin gewerkt aan een aantal aanbevelingen voor een effectief Europees anti-witwasbeleid:

- één Europese Regulation in plaats van Directives (dat is dwingender);
- beperking van de discretionaire bevoegdheden van de lidstaten;
- level playing field op wereldschaal bij de strijd tegen het witwassen;
- sterkere rol **European Banking Authority (EBA)** bij regelgeving;
- harmonisering van het toezicht (grensoverschrijdende coördinatie); dat geldt ook voor het werk van de Financial Intelligence Units;
- meer informatiedeling tussen banken en tussen publieke en private instellingen, met respect voor de privacywetgeving;
- transparante en zorgvuldige UBO-registratie.

De eerste voorstellen van de Europese Commissie kunnen we in de komende weken verwachten, en zullen nauwlettend worden opgevolgd.

Trends op vlak van witwassen en financiering van terrorisme²



De praktijk van het witwassen is aan voortdurende verandering onderhevig. Is de ene modus operandi verhinderd, wordt er weer een andere creatieve manier gevonden om de criminele oorsprong van vermogen en middelen te verhullen. Het blijft een waar kat-en-muisspel.

De COVID-19-crisis had weliswaar een vertragende impact op de economie, helaas niet op fraudeurs en hun werkzaamheden. Integendeel, in deze periode werden verschillende nieuwe fraudetrends vastgesteld, waarbij handig werd ingespeeld op de actualiteit en die bijkomende uitdagingen met zich mee hebben gebracht voor de banksector op het vlak van de bestrijding van witwassen en financiering van terrorisme.

² Bron: Jaarverslag CFI 2020: [jv2020.pdf](#) (ctif-cfi.be)

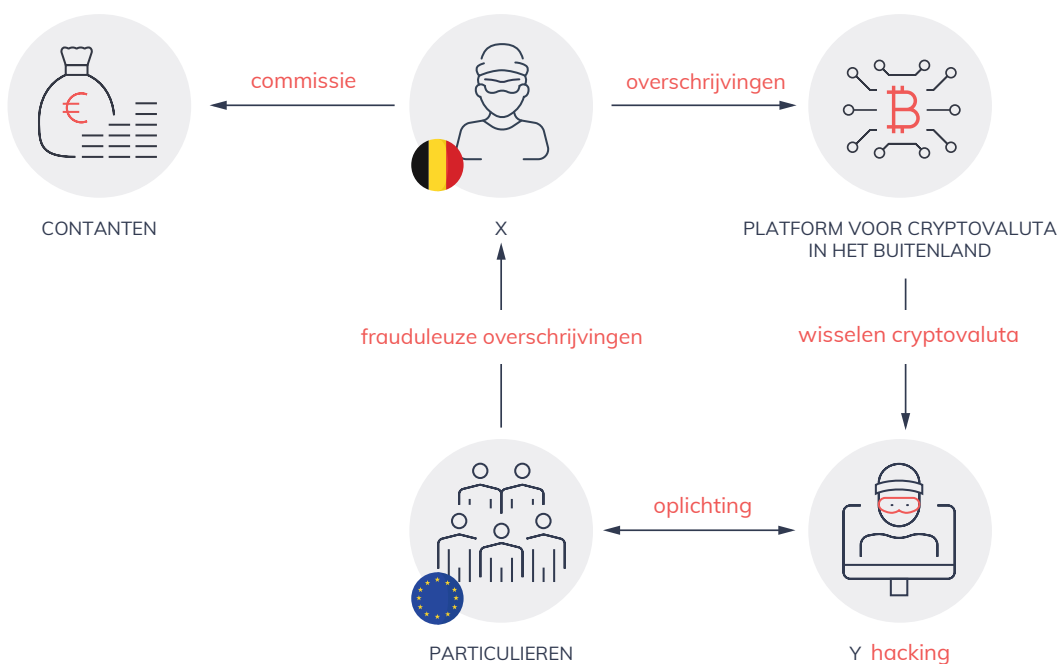
Zo is het aantal **phishingmails** waarbij cybercriminelen, in naam van een financiële instelling of andere autoriteiten, vragen om de beveiligingsgegevens van je kaart bij te werken- onder het voorwendsel van de uitzonderlijke situatie waarin we ons bevinden- enorm gestegen en werd de 'visvijver' van potentiële slachtoffers nog groter.

Uit **statistieken van Febelfin** blijkt dat in 2020 ongeveer **67 000 frauduleuze transacties via phishing** hebben plaatsgevonden, voor een totaal nettobedrag van ongeveer **34 miljoen euro**.

Alarmerend is dat **steeds meer geldezels** worden ingezet om crimineel verkregen geld vlug en gemakkelijk van de ene naar de andere rekening te kunnen doorsluizen.

Momenteel is het nog niet mogelijk voor banken om persoonsgegevens inzake fraude uit te wisselen omwille van (privacy)wetgeving. Banken blijven op dit vlak zeer voorzichtig omdat zij door de toezichthouders en wetgeving aan zeer strikte reglementering gebonden zijn. Febelfin onderzoekt de mogelijkheid om op wettelijke basis een systeem op te richten voor het uitwisselen van identiteitsgegevens van geldezels tussen financiële instellingen.

Ook **beleggingsfraude** (online reclame voor valse beleggingsvormen) en **fraude via cryptovaluta** nemen steeds grotere proporties aan. De meeste fraudemeldingen bij beleggingen gaan over **boiler rooms, recovery rooms en binaire opties**. Bij fraude via cryptovaluta spelen **geldezels** ook een grote rol. Ze krijgen (crimineel verkregen) geld op hun bankrekening gestort waarmee ze cryptovaluta moeten aankopen. In de illustratie hieronder wordt duidelijk hoe alles in zijn werk gaat.



Voorbeeld van hoe geldezels werken en hoe witwassen met cryptovaluta gebeurt: bron CFI

EEN GREEP UIT HET OPLEIDINGSAANBOD VAN FEBELFIN ACADEMY



Febelfin Academy heeft een breed aanbod van basisopleidingen, advanced en expert opleidingen, in verschillende leervormen (e-learning – klassikaal – blended) en in co-creatie met verschillende partners. Nieuw sinds dit jaar is dat ze nu ook een focus leggen op hoe je de theorie/wetgeving toepast in de dagelijkse relatie met de klant.

Kennisvereisten bij start in het beroep

Elke medewerker bank/verzekeringen/kredieten die in contact komt met een klant, moet zijn/haar kennis kunnen bewijzen. Dit is gebaseerd op wettelijke initiatieven en ook hier wordt AML in opgenomen.

Dit betekent bijvoorbeeld dat een medewerker in een garage deze kennis moet bewezen hebben om een autolening te kunnen aanbieden.

- Bankbemiddeling (Wet Willems)
- Verzekeringsdistributie IDD
- Kredietbemiddeling

PERMANENTE BIJSCHOLING

Basisopleidingen

Deze opleidingen richten zich tot elke medewerker die in zijn/haar dagelijkse functie in contact komt met AML.

Basisopleiding met als objectief een algemeen beeld te schetsen van AML.
Belang en impact:

- De strijd tegen witwassen (AML) en terrorismefinanciering (CFT): algemene module + Beleggingsfondsen + Betalingsdiensten en Elektronisch Geld
- Witwasregelgeving (AML V) verplichtingen - een globaal overzicht

Toepassing van de AML in de praktijk en in onze relatie met de klant: focus op handelsvaardigheden:

- Anti Money Laundering (AML) en Know your Customer (KYC) in de relatie en contacten met klanten

Advanced opleidingen

De focus wordt gelegd op de verdieping van de AML-kennis en -toepassing in de organisatie en haar processen. Deze opleidingen richten zich hoofdzakelijk tot medewerkers die in belangrijke mate met de AML-materie werken.

Advanced opleiding met als doel de actoren van terrorismefinanciering te herkennen en ertegen op te treden, en dit vanuit de praktijk toegelicht door een federal crime detective commissioner:

- Preventie van terrorismefinanciering
- Het leren herkennen van witwastypologieën

Advanced opleiding die verdieping biedt in de historiek en het algemeen wettelijk kader:

- Anti-witwassen van geld: AML V

Belang van AML in het kader van verzekeringen:

- Bijscholing verzekering leven - Aanbod van levensverzekeringen: de precontractuele verplichtingen van de AML-wet, van het WER en van de IDD

Expert opleidingen

De focus ligt op de impact van AML op het beleid van de organisatie in haar verschillende aspecten. Deze opleidingen richten zich tot medewerkers die mee het beleid uitwerken van de organisatie. Er gaat ook aandacht naar de toekomstige en strategische impact.

AML en cryptocurrencies:

- [Investing in bitcoins or other cryptocurrencies: prudential framework](#)

Sancties en embargo's in het kader van AML:

- [AML: Sancties en embargo's](#)

AML en rol van de Raad van Bestuur:

- [Executive program - The Board of Directors in the Financial Sector](#)

Wat betekent AML voor onze privacy en hoe gaan we hiermee om in onze organisatie?

- [Developments for AML and challenges with Privacy: the perfect storm?](#)

Certificatieprogramma in samenwerking met Deloitte Regulatory Services ter voorbereiding op het examen van Certified compliance officer:

- [Traject - Certified Compliance Officer](#)

Hoe risk assessment uitwerken voor de organisatie?

- [Praktische organisatie en aanpak van risicobeoordeling binnen compliance](#)



Belgische Federatie van de financiële sector

www.febelfin.be