Febelfin-actieplan voor de aanpak van online fraude

Samenvatting

Febelfin en haar leden delen ten volle de bezorgdheid over de groeiende impact van online fraude op consumenten en op de samenleving als geheel. Door de digitalisering, technologische innovatie, steeds geavanceerdere social engineering-technieken en de opkomst van criminele netwerken is online fraude uitgegroeid tot een structurele maatschappelijke uitdaging die snel evolueert.

De afgelopen jaren is het aantal fraudepogingen sterk toegenomen, en zijn de gebruikte technieken steeds geavanceerder geworden. **Daarom leveren banken aanzienlijke en blijvende inspanningen om fraude beter te voorkomen en op te sporen, en klanten beter te beschermen.** Deze inspanningen zijn gericht op alle aspecten van fraude, van preventie en voortdurende transactiemonitoring tot operationele beveiligingsmaatregelen, samenwerking met politie en justitie en permanente sensibilisering van klanten.

Deze inspanningen zijn de afgelopen jaren enorm toegenomen (meer IT-ontwikkelingscapaciteit, meer anti-fraudemedewerkers, …). Dit toont aan dat de financiële sector zich ten volle engageert om haar rol in de strijd tegen online fraude op te nemen. Banken zullen hun technische en operationele beveiligingsmaatregelen verder uitbreiden, de samenwerking met andere banken en andere relevante stakeholders verder verdiepen – met de nodige steun van beleidsmakers en regelgevende instanties – en de ondersteuning van klanten bij fraude blijven verbeteren. Tegelijkertijd erkent de sector dat banken deze uitdaging niet alleen kunnen aangaan.

Online fraude kan niet doeltreffend worden bestreden met een aanpak die uitsluitend op banken is gericht. Een duurzame bestrijding van fraude vereist **een geïntegreerde en gecoördineerde aanpak waarin alle actoren in de fraudeketen hun verantwoordelijkheid nemen**, met de overheid in een sleutelrol als coördinator en facilitator. Fraude moet zo dicht mogelijk bij de bron worden aangepakt, met name door nauwere samenwerking met telecomoperatoren en sociale media platformen, en door een doeltreffend onderzoeks- en vervolgingsbeleid om georganiseerde criminele netwerken te stoppen. Net als in de buurlanden is een collectieve en gestructureerde aanpak essentieel om deze vorm van georganiseerde misdaad te bestrijden. Zo vermijden we dat België een aantrekkelijk doelwit wordt voor fraudeurs.

Belgian Financial Sector Federation vzw/asbl
Boulevard du Roi Albert II 19 - 1210 Brussels
http://www.febelfin.be | T + 32 2 507 68 11 | F + 32 2 888 68 11
Governance Note FEB559746
Last saved on 7/07/2026 15:40:00 – 23 pages

Tegen deze achtergrond stellen Febelfin en haar leden een uitgebreid actieplan voor dat is opgebouwd op basis van drie complementaire niveaus.

1. **Banken verbinden zich er individueel toe operationele en technische beveiligingsmaatregelen te nemen, gericht op het verder versterken van de preventie, detectie en aanpak van fraude. Dit houdt de invoering in van een aantal 'slow banking'-maatregelen, waarbij een voldoende evenwicht tussen veiligheid en gebruiksvriendelijkheid wordt gehandhaafd.**

2. **Banken zullen de interbancaire samenwerking versterken** en streven naar een meer geïntegreerde aanpak, waarbij gegevens worden gedeeld en gemeenschappelijke technologische voorzieningen worden ingezet. De financiële sector verbindt zich er ook toe om de dienstverlening aan klanten meer te harmoniseren en klantgerichter te maken, alsook in te zetten op gezamenlijke bewustmaking.

3. **Banken pleiten voor een aanpak door het volledige ecosysteem**, aangezien fraude vaak al in een vroeger stadium begint – via telecomoperatoren, sociale media platformen en digitale kanalen – en dat dit een grotere betrokkenheid en verantwoordelijkheid van andere stakeholders vereist, evenals doeltreffende wetshandhaving.

Deze drieledige aanpak, die **brede maatschappelijke en regelgevende steun** vereist, heeft tot doel de **consumenten nog beter te beschermen**, de operationele doeltreffendheid te verbeteren en aan te sluiten bij het Europese regelgevingskader dat in ontwikkeling is, met de Payment Services Regulation (PSR). Daarnaast onderstreept deze aanpak het belang van sterke **politieke steun** om gegevensdeling mogelijk te maken, sectoroverschrijdende verantwoordelijkheid te waarborgen en versnippering in de regelgeving te vermijden. Alleen door **samen te werken met alle stakeholders in het ecosysteem**, kunnen we uiteindelijk een **duurzame bestrijding** van online fraude mogelijk maken.

Inleiding: het huidige fraudelandschap

Febelfin en haar leden nemen de strijd tegen online fraude bijzonder ernstig. De sector is zich ten volle bewust van de financiële, emotionele en maatschappelijke impact van fraude op slachtoffers. Banken investeren dagelijks middelen om fraude te voorkomen, verdachte activiteiten op te sporen, frauduleuze transacties te blokkeren, waar mogelijk gelden te recupereren, slachtoffers te ondersteunen, en nauw samen te werken met de overheid en de politiediensten. Die inspanningen worden voortdurend aangepast aan nieuwe fraudepatronen en bedreigingen.

Ondanks die blijvende inspanningen veroorzaakt online fraude nog steeds **aanzienlijke schade**. In 2025 slaagden fraudeurs erin om 93 miljoen euro buit te maken via phishing. Dit cijfer toont de hardnekkigheid en het aanpassingsvermogen van criminele netwerken aan.

Tegelijkertijd is het belangrijk om online fraude in haar bredere context te plaatsen. In verhouding tot het totale transactievolume vertegenwoordigt het nettoverlies door fraude ongeveer 0,004% van het totale transactiebedrag (2025). Dat toont aan dat frauduleuze transacties relatief beperkt blijven, maar ook dat fraude een grote impact kan hebben op individuele slachtoffers en dat blijvende inspanningen nodig zijn om consumenten beter te beschermen, want elk slachtoffer is er één te veel.

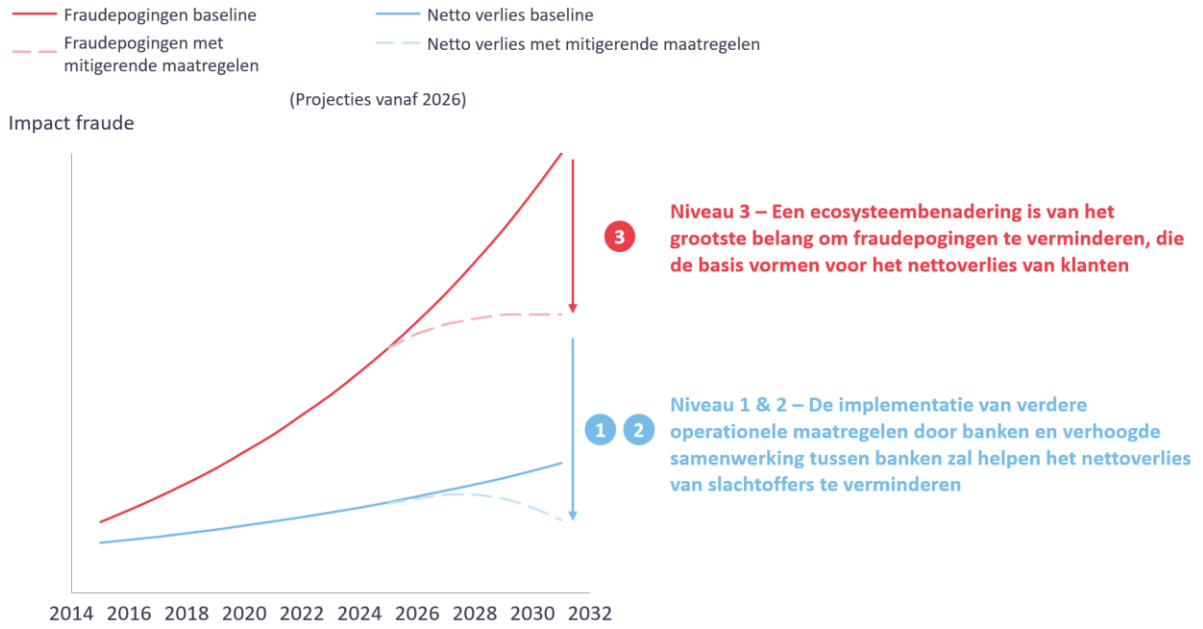
Online fraude is **fundamenteel veranderd**. Verschillende stakeholders uit het hele ecosysteem zijn betrokken in de fraudeketen. Criminelen werken steeds georganiseerder en op grotere schaal. Daarbij maken ze gebruik van phishingkits, valse websites, geldezels, callcenters en zogenaamde scam farms. Ook zetten ze advertenties op sociale media in, gebruiken ze software om toestellen vanop afstand over te nemen en maken ze steeds vaker gebruik van artificiële intelligentie. Telecomoperatoren, sociale media platformen, marktplaatsen en andere digitale kanalen worden vaak al in een vroeg stadium gebruikt om slachtoffers te zoeken, te contacteren en te manipuleren.

Banken zijn daarentegen vooral betrokken in een latere fase. Ze verwerken en monitoren transacties, nemen preventieve en opsporingsmaatregelen, blokkeren betaalinstrumenten indien nodig, starten recuperatieacties en begeleiden klanten na fraude. Die rol is essentieel, maar betekent ook dat **banken weinig invloed hebben op de eerste fase van fraude**, waarin slachtoffers al worden benaderd en gemanipuleerd nog vóór er een betaling wordt geïnitieerd.

Banken beschikken vandaag al over **een breed en robuust pakket aan operationele en technische maatregelen** om klanten te beschermen tegen online fraude. Die maatregelen houden rekening met de verschillende aspecten van fraude en hebben elk een andere, maar complementaire impact op de fraudedynamiek. Enerzijds zijn er **preventiemaatregelen**, zoals sterke klantauthenticatie, itsme® en de verificatie van de naam van de begunstigde, die fraude helpen beperken door pogingen moeilijker te maken. Anderzijds nemen banken **detectie- en mitigatiemaatregelen**, zoals transactiemonitoring, het blokkeren van verdachte transacties, waarschuwingen en acties om gestolen geld waar mogelijk terug te halen. Die maatregelen zijn in de eerste plaats gericht op het beperken van de financiële impact van fraude door verliezen te beperken na een succesvolle fraudepoging.

Deze maatregelen leveren vandaag al tastbare resultaten op en versterken de bescherming van klanten. Door hun preventie-, detectie- en reactievermogen voortdurend te verbeteren, zijn banken steeds beter in staat om verdachte transacties te herkennen, in realtime in te grijpen en financiële verliezen voor klanten te beperken. Banken blijven zich ten volle engageren om deze inspanningen verder te versterken, onder meer via bijkomende operationele maatregelen, technologische innovatie en nauwere samenwerking binnen de sector. Deze blijvende investeringen zijn cruciaal om de financiële impact van fraude verder te beperken en slachtoffers beter te beschermen.

De evolutie van de fraudedynamiek, zoals weergegeven in de grafiek hieronder, toont echter aan dat deze maatregelen vooral een impact hebben op de **gevolgen van fraude zodra die zich voordoet**, en minder op het **totale aantal fraudepogingen**. Zelfs wanneer banken hun maatregelen verder versterken, blijft hun vermogen om het aantal aanvallen structureel terug te dringen beperkt. Fraude ontstaat immers grotendeels vroeger in de keten, via kanalen buiten de banksector. **Een duurzame en significante daling van fraude hangt daarom in grote mate af van doeltreffende acties binnen het bredere ecosysteem** — met name door telecomoperatoren, sociale media platformen, digitale dienstverleners en ordediensten — om frauduleuze activiteiten bij de bron te voorkomen, op te sporen en te verstoren. Bijkomende bankmaatregelen zijn noodzakelijk, maar alleen een gecoördineerde aanpak binnen het volledige ecosysteem kan de evolutie van het aantal fraudepogingen wezenlijk veranderen.



Deze evolutie van fraude hangt nauw samen met bredere **digitale trends.** De snelle opmars van digitaal en mobiel bankieren en instantbetalingen vergroot het gebruiksgemak voor consumenten, maar brengt ook nieuwe kwetsbaarheden met zich mee. Fraudeurs spelen hierop in en ruilen massale phishing vaak in voor gerichte aanvallen, waarbij ze gebruikmaken van geavanceerde dataverzameling, artificiële intelligentie, deepfake-stemmen en overtuigende phishingberichten in verschillende talen.

Steeds vaker richten fraudeurs zich rechtstreeks tot klanten, waarbij ze vertrouwen, urgentie en manipulatie uitbuiten om slachtoffers ertoe te brengen zelf hun gegevens te delen, transacties goed te keuren of overschrijvingslimieten te verhogen. In dergelijke gevallen kan de bank op het moment van uitvoering niet meteen het fraudegeval herkennen, maar ziet ze een transactie die door de klant lijkt te zijn goedgekeurd. Deze fraudevormen, waarbij slachtoffers zelf transacties goedkeuren, winnen aan belang omdat ze traditionele beveiligingsmaatregelen kunnen omzeilen. Ze tonen ook de grenzen van controles door de banken aan en onderstrepen de nood aan een bredere, geïntegreerde aanpak om fraude bij de bron te bestrijden (zie bijlage voor twee voorbeelden van het fraudeverloop bij de meest voorkomende modi operandi).

Dit toont duidelijk aan dat samenwerking noodzakelijk is. Banken moeten hun eigen controles verder blijven versterken, maar een louter bankgerichte aanpak volstaat niet. **Fraude moet over de volledige keten worden aangepakt**, via sterkere preventie in een vroeg stadium, betere gegevensdeling, duidelijkere verantwoordelijkheden voor andere sectoren, een meer doeltreffende handhaving, meer coördinatie en een coherente nationale aanpak.

Tegen deze achtergrond stelt Febelfin een ambitieus maar operationeel realistisch actieplan voor, waarbij banken belangrijke bijkomende engagementen aangaan en tegelijk expliciet pleiten voor een gecoördineerde en geïntegreerde aanpak in het volledige ecosysteem. **Het doel is om klanten nog beter te beschermen, de preventie en aanpak van fraude doeltreffender te maken, en volledig in overeenstemming te blijven met het huidige en toekomstige Europese regelgevende kader**, waaronder PSD2, de Instant Payments Regulation en de toekomstige Payment Services Regulation. Nationale initiatieven moeten immers in overeenstemming blijven met dat Europese kader en goldplating moet worden vermeden.

Febelfin actieplan niveau 1 – Operationele en technische maatregelen die door individuele banken worden genomen en verder worden versterkt

Banken beschikken vandaag al over **een breed en robuust pakket aan operationele en technische maatregelen** om klanten te beschermen tegen online fraude.

De voorbije jaren hebben banken hun inspanningen verder aangescherpt door extra **menselijke en technologische middelen** in te zetten. Zo breidden ze zowel hun IT-ontwikkelingscapaciteit als hun gespecialiseerde fraudeteams uit. Dat weerspiegelt zowel de structurele aard van de dreiging als de nood om zich voortdurend aan te passen aan evoluerende fraudepatronen.

Als aanvulling op de reeds bestaande maatregelen die de individuele banken nemen op basis van hun klantenbestand en risicoprofiel, **verbinden zij zich ertoe hun eigen kader verder te versterken met een reeks operationele maatregelen**. Het doel is om **binnen de sector een gemeenschappelijke basis** te creëren, met een **basispakket aan operationele maatregelen** waartoe alle banken zich verbinden. Banken zullen die maatregelen daarnaast implementeren en verder blijven aanvullen op basis van hun eigen risicoprofiel en de specifieke kenmerken van hun klantenbestand, rekening houdend met de beoogde timing voor elke maatregel.

De voorgestelde maatregelen zijn niet alleen bedoeld om de **technische bescherming te versterken**, maar ook om waar nodig bewust **momenten van vertraging en reflectie** in te bouwen in het transactieproces, **zodat fraudescenario's kunnen worden verstoord**. Door bepaalde risicovolle stappen te **vertragen** — bijvoorbeeld via cooling-downmechanismen — en klanten via gerichte waarschuwingen en bevestigingen bewuster te maken, willen banken de **fraudeketen op cruciale momenten doorbreken**.

Deze maatregelen houden rekening met de belangrijkste kenmerken van hedendaagse fraude — urgentie, manipulatie en transacties met hoge bedragen — en streven tegelijk naar een proportioneel evenwicht tussen veiligheid, gebruiksgemak en de autonomie van de klant.

Het Febelfin actieplan omvat de volgende operationele maatregelen die individuele banken nemen, met als doel:

Online fraude te voorkomen:

1. **Verlaging van de standaardlimiet (5.000 euro/dag) voor overschrijvingen vanaf betaalrekeningen voor retailklanten**
2. **Cooling-downperiode (>4 u) bij limietverhoging**
3. **Melding bij limietverhoging**
4. **Contextuele ondertekening**[1]
5. **Keuzevrijheid tussen instant- en standaard overschrijvingen**
6. **Beperking frauduleuze transacties op spaarrekeningen**

Online fraude te detecteren en aan te pakken:

7. **Versterking van fraudedetectie en transactiemonitoring**
8. **Detectie van malware en remote access tools (RAT)**

Online fraude voorkomen:

1. Verlaging van de standaardlimiet (5.000 euro/dag) voor overschrijvingen vanaf betaalrekeningen voor retailklanten – beperking van de financiële blootstelling

Aantal banken dat vandaag al de lagere standaardlimiet toepast (op basis van een steekproef van 10 retailbanken, 4/10)

Banken zullen de **standaardlimiet voor overschrijvingen vanaf betaalrekeningen voor retailklanten verlagen tot maximaal 5.000 euro per dag**. Een lager standaardplafond **beperkt de maximale financiële blootstelling per fraudegeval**, met name wanneer verliezen voortvloeien uit één enkele transactie met een hoog bedrag. Door de standaardlimieten te verlagen, wordt het bedrag dat fraudeurs kunnen buitmaken zonder de limiet te verhogen aanzienlijk beperkt. Klanten zullen een verhoging kunnen aanvragen, maar daarvoor zullen gecontroleerde procedures en bijkomende beveiligingsmaatregelen gelden (zie cooling-downperiode en meldingen).

De standaardlimiet bedraagt maximaal 5.000 euro per dag. Een bank kan er altijd voor kiezen een strengere standaardlimiet toe te passen (bijvoorbeeld 4.000 euro per dag of 5.000 euro per week).

[1] Contextuele ondertekening waarborgt dat de transactiegegevens die aan de rechtmatige ondertekenaar worden getoond (inclusief het bedrag en het volledige IBAN-nummer van de begunstigde) dezelfde zijn als de transactiegegevens die effectief worden uitgevoerd. Dit omvat ook ondertekeningsmiddelen die rechtstreeks aan een toestel zijn gekoppeld, zoals Face ID/vingerafdruk op mobiele toestellen en passkeys.

Het is ook belangrijk te benadrukken dat klanten hun persoonlijke limieten zelf lager kunnen instellen dan de standaardlimiet die de bank heeft ingevoerd.

Beoogde timing: Q1 2027

2. **Cooling-downperiode (>4 u) bij limietverhoging – vertraging inbouwen en fraudescenario's verstoren**

Aantal banken dat vandaag al de cooling-downperiode toepast (op basis van een steekproef van 10 retailbanken, 5/10)

Banken zullen **een cooling-downperiode (van minstens 4 uur) invoeren** bij verhogingen van overschrijvingslimieten. Concreet betekent dit dat een aanvraag om de overschrijvingslimiet van een klant via digitale kanalen te verhogen, niet onmiddellijk in werking treedt. In de plaats daarvan blijft de vorige, lagere limiet nog minstens 4 uur actief. Die maatregel is bedoeld om fraudescenario's te verstoren die inspelen op urgentie en een onmiddellijke uitvoering zodra de limiet is verhoogd.

Beoogde timing: Q4 2026, met een zorgvuldige afstemming om hinder bij legitieme dringende betalingen zo veel mogelijk te beperken.

3. **Melding bij limietverhoging – een tweede verdedigingslinie voor snelle detectie**

Aantal banken dat vandaag al de melding bij limietverhoging toepast (op basis van een steekproef van 10 retailbanken, 7/10)

Banken zullen **systematisch realtime meldingen verzenden wanneer overschrijvingslimieten worden verhoogd** (en wanneer de cooling-downperiode is afgelopen). Dit voegt een bijkomende beveiligingslaag toe, aangezien klanten onmiddellijk worden gewaarschuwd voor een wijziging die mogelijk het gevolg is van manipulatie. Deze meldingen moeten duidelijk, praktisch en actiegericht zijn (wat is gewijzigd, wanneer is dat gebeurd, en wat moet de klant doen als hij/zij die wijziging niet zelf heeft aangevraagd).

Beoogde timing: Q2 2027

4. **Contextuele ondertekening – frauderisico verminderen**

Aantal banken dat vandaag al de contextuele ondertekening toepast (op basis van een steekproef van 10 retailbanken, 4/10)

Banken zullen de bevestiging van transacties nog veiliger maken door klanten op het moment van goedkeuring duidelijke informatie over de transactie te tonen, zoals het bedrag en de gegevens van de begunstigde. Dat helpt klanten om **exact te begrijpen wat zij goedkeuren** en verkleint het risico dat zij onder manipulatie onbewust een frauduleuze transactie goedkeuren.

De invoering zal **geleidelijk gebeuren in de periode 2026-2027**. Deze maatregel houdt ook in dat kaartlezers waarbij contextuele ondertekening niet mogelijk is, geleidelijk worden uitgefaseerd. Klanten die dat wensen, zullen deze kaartlezers wel kunnen blijven gebruiken.

5. **Keuzevrijheid tussen instant- en standaard overschrijvingen – beperking van het frauderisico**

Aantal banken dat vandaag al de keuzevrijheid tussen instant- en standaard overschrijvingen biedt
(op basis van een steekproef van 10 retailbanken, 10/10)

Banken zullen ervoor zorgen dat klanten altijd kunnen kiezen tussen een instant overschrijving en een standaard overschrijving. Sinds oktober 2025 zijn alle banken in Europa verplicht om hun klanten instant betalingen aan te bieden. Instant betalingen, waarbij gelden binnen enkele seconden op de rekening van de begunstigde staan, winnen aan populariteit door hun snelheid en gebruiksgemak. Fraudeurs kunnen de onmiddellijke uitvoering van deze betalingen misbruiken om, zodra een slachtoffer in de val werd gelokt, geld zeer snel van zijn/haar rekening weg te sluizen.

Om dat risico te beperken, **zullen banken klanten altijd de mogelijkheid bieden om voor een standaard overschrijving te kiezen**, waarbij het bedrag niet onmiddellijk op de rekening van de begunstigde wordt gestort. Dat extra tijdsvenster kan fraudescenario's die inspelen op urgentie en druk helpen doorbreken, en biedt meer ruimte om verdachte situaties tijdig op te sporen of opnieuw te beoordelen vóór er onherstelbare schade ontstaat.

Die **keuzevrijheid** kan, afhankelijk van de bank, op verschillende manieren worden ingevuld:

- de bank kan de standaardoverschrijving als standaardoptie aanbieden, waarbij de klant expliciet voor een instant betaling kiest als hij of zij dat wenst;
- de bank kan de instant betaling als standaardoptie aanbieden, met de mogelijkheid voor de klant om over te schakelen naar een standaardoverschrijving;
- de bank kan de klant vragen om bij elke transactie te kiezen tussen een instant- of een standaardoverschrijving.

De klant behoudt steeds de volledige controle en kan kiezen welke overschrijving het best aansluit bij zijn/haar behoeften. Deze maatregel wil gebruiksgemak en bescherming met elkaar verzoenen doordat klanten een **weloverwogen en geïnformeerde keuze** kunnen maken. Zo **worden fraudescenario's vertraagd en kan de fraudeketen worden doorbroken**, waarbij een proportioneel evenwicht tussen snelheid, veiligheid en gebruiksgemak wordt vooropgesteld.

Beoogde timing: onmiddellijk (Q2 2026)

6. Beperking frauduleuze transacties op spaarrekeningen

Aantal banken dat vandaag al maatregelen neemt om frauduleuze transacties op spaarrekeningen te beperken (op basis van een steekproef van 10 retailbanken, 2/10)

Banken zullen bijkomende maatregelen nemen om frauduleuze transacties op spaarrekeningen te beperken. Die maatregelen kunnen er als volgt uitzien:

- retailklanten de mogelijkheid bieden om online overschrijvingen van hun gereglementeerde spaarrekening naar hun betaalrekening te beperken en/of te blokkeren — als onderdeel van een 'slow banking'-aanpak — in combinatie met een veilig alternatief om dergelijke transacties toe te staan (bv. verwerking in het kantoor of een aanvullende cooling-downperiode); en/of
- Een dynamische optie invoeren om transacties tijdelijk 'on hold' te zetten op basis van transactiemonitoring.

Beoogde timing: Q3 2027

Detectie & aanpak van online fraude

7. Versterking van fraudedetectie en transactiemonitoring

Banken zullen hun maatregelen om frauduleuze transacties op te sporen en te voorkomen versterken door hun **capaciteit op het vlak van fraudedetectie en transactiemonitoring** nog verder uit te breiden. Geavanceerde monitoringsmechanismen maken het mogelijk om verdachte patronen te herkennen en, waar nodig, tijdig in te grijpen door mogelijk frauduleuze transacties te blokkeren of tijdelijk tegen te houden vóór er onherstelbare schade ontstaat.

Daarnaast is het essentieel dat er een **aangepast kader komt om mogelijke juridische of regelgevende belemmeringen weg te nemen** die het gebruik van doeltreffende fraudedetectietools kunnen beperken, zoals transactiemonitoring op basis van gedrag met behulp van geavanceerde analysetechnieken. Technologische innovatie kan een krachtig instrument zijn in de strijd tegen online fraude, op voorwaarde dat ze op een verantwoorde en proportionele manier wordt ingezet.

Banken benadrukken daarom het belang om dergelijke innovatie toe te laten binnen een **duidelijk en rechtszeker kader**, met volledige naleving van de geldende regels inzake privacy en gegevensbescherming. Het juiste evenwicht tussen doeltreffende fraudepreventie, technologische vooruitgang en de bescherming van fundamentele rechten is essentieel om klanten beter te beschermen en fraude over de volledige transactieketen tegen te gaan. De invoering zal **geleidelijk gebeuren in de periode 2026-2028**.

8. **Detectie van malware en remote access tools (RAT) – gericht op de meest geavanceerde fraudetechnieken**

Aantal banken dat vandaag al de detectie van malware en remote access tools (RAT) inzet (op basis van een steekproef van 10 retailbanken, 4/10)

Banken zullen verder onderzoeken welke mechanismen kunnen helpen om verdachte situaties tijdens het online bankieren op te sporen (bv. via de detectie van malware of software waarmee fraudeurs een toestel vanop afstand kunnen overnemen). Dit is een belangrijk onderdeel van de strijd tegen meer geavanceerde fraudetechnieken. De ontwikkeling en afstemming van deze mechanismen moet zorgvuldig gebeuren, onder meer om het aantal 'false positives' zo beperkt mogelijk te houden en ervoor te zorgen dat de impact op de klant proportioneel blijft. **De invoering zal geleidelijk gebeuren in de periode 2026-2028.**

Tot slot is online fraude een evolutief fenomeen dat permanent moet opgevolgd worden en waarbij best practices voortdurend worden geïdentificeerd, geëvalueerd en ingevoerd indien doeltreffend tegen online fraude. Inspiratie kan hierbij ook uit het buitenland gehaald worden, waar soms instrumenten of maatregelen worden ingevoerd die niet altijd gebaseerd zijn op Europese regelgeving. Febelfin engageert zich om via benchmarking nieuwe features te identificeren, te evalueren en haar leden aan te bevelen om ze in te voeren wanneer ze doeltreffend zijn en een draagvlak krijgen binnen de sector.

Bij het invoeren van bovenstaande maatregelen moet worden in acht genomen dat al deze technische en operationele aanpassingen, die een vorm van "slow banking" invoeren, een impact hebben op de klant. Ze versterken de bescherming, maar kunnen bij bepaalde transacties ook zorgen voor extra stappen of vertragingen. Febelfin benadrukt daarom dat **brede maatschappelijke en politieke steun noodzakelijk is**. Sterkere beschermingsmaatregelen kunnen alleen werken en duurzaam zijn als klanten, beleidsmakers en toezichthouders erkennen dat meer veiligheid soms ook aanpassingen vraagt op het vlak van snelheid, gebruiksgemak en klantervaring.

Febelfin actieplan niveau 2 – Samenwerking tussen banken

Maatregelen op het niveau van de individuele banken zijn noodzakelijk, maar niet voldoende. Bij online fraude zijn vaak verschillende banken betrokken, zeker wanneer fraudeurs geldezels inzetten of bedragen snel doorsluizen via verschillende banken en landen. Een **sterkere samenwerking tussen banken** is daarom essentieel om fraude sneller op te sporen, geld sneller te blokkeren, de recuperatie van geld te verbeteren en slachtoffers een meer consistente en klantgerichte ondersteuning te bieden.

In het Febelfin actieplan zijn de volgende maatregelen op het vlak van de samenwerking tussen banken opgenomen:

Online fraude voorkomen:

1. **Fraudstop**
2. **Sensibiliseringcampagnes**
3. **Itsme ®**

Online fraude detecteren en aanpakken:

4. **Platform voor het delen van fraudegegevens**
5. **Communicatiecharter – engagement van de banksector om fraudedossiers binnen 15 bankwerkdagen te behandelen**

Online fraude voorkomen:

1. Fraudstop – één centraal meldpunt dat 24/7 bereikbaar is

Slachtoffers weten in de eerste minuten nadat ze fraude ontdekken vaak niet wat ze moeten doen: wie ze moeten bellen, welke stappen ze moeten volgen en wat het meest dringend is. Daarom ontwikkelde de sector Fraudstop: **één centraal meldpunt met het nummer (078 170 170)** dat dag en nacht, zeven dagen op zeven bereikbaar is. Via Fraudstop worden slachtoffers snel doorverwezen naar hun bank en wordt alles in het werk gesteld om de nodige beschermingsmaatregelen te nemen, zoals het blokkeren van betaalmiddelen wanneer dat nodig is. Dit initiatief bouwt voort op de bekendheid en sterkte van Card Stop en heeft als doel slachtoffers op een snellere en eenvoudigere manier hulp te bieden. Naast dit nieuwe meldpunt blijft elke bank bereikbaar via haar bestaande fraudekanalen.

Timing: gelanceerd op 22 juni 2026.

2. Sensibiliseringscampagnes – regelmatige communicatie naar het brede publiek

Banken zullen blijven investeren in sensibiliseringscampagnes. Omdat fraudeurs bij veel vormen van online fraude inspelen op menselijk gedrag en gebruik maken van social engineering, is de **weerbaarheid van klanten een essentieel onderdeel van preventie**.

Sensibiliseringsinitiatieven moeten regelmatig worden herhaald, gericht zijn op specifieke fraudevormen en afgestemd worden op de gebruikte communicatiekanalen. Idealiter gebeurt sensibilisering via een gezamenlijke inspanning van het volledige ecosysteem, zodat de initiatieven meer impact en een groter bereik hebben. Banken steunen het idee om grootschalige sensibiliseringscampagnes te ontwikkelen, naar analogie met de bekende BOB-campagnes.

Beoogde timing: periodiek.

3. itsme® zal zijn fraudepreventiemaatregelen versterken

De afgelopen acht jaar heeft itsme® zijn fraudepreventie voortdurend verder uitgebouwd, onder meer door bijkomende datapunten toe te voegen en specifieke mitigerende maatregelen te ontwikkelen, in nauwe afstemming met de banken. Sommige maatregelen gebeuren via een rechtstreekse integratie met de banken, waarbij relevante signalen worden uitgewisseld. Andere innovaties zijn duidelijk zichtbaar voor gebruikers en zorgen onmiddellijk voor contextuele bewustmaking.

Als onderdeel van deze initiatieven zal itsme® **extra beveiligingslagen toevoegen via itsme® en via innovaties in mobiele apps.** Dat moet het risico op accountovername verminderen en voorkomen dat fraudeurs namens hun slachtoffers een login of betaling bevestigen. Alleen de echte gebruiker, van wie het gezicht overeenkomt met de foto op zijn of haar Belgische identiteitskaart, zal kunnen optreden als rekeninghouder. Dat creëert een bijkomende beveiliging die fraudeurs niet kunnen omzeilen. **Beoogde timing: Q1 2027**

Online fraude detecteren en behandelen:

4. Platform voor het delen van fraudegegevens – een netwerkgebaseerd informatiesysteem

Een belangrijk initiatief is de ontwikkeling van een **platform voor het delen van fraudegegevens via Isabel en itsme®.**

Banken willen fraudesignalen sneller en op een meer gestructureerde manier delen, zodat verdachte patronen vroeger kunnen worden herkend en gestopt. Het doel is om te evolueren van afzonderlijke detectie per bank naar een aanpak op basis van **gedeelde inzichten binnen het netwerk**. Door relevante fraude-indicatoren te delen, kunnen banken geldezels sneller opsporen, meer frauduleuze transacties voorkomen en hun aanpak beter op elkaar afstemmen. In die context is de verdere ontwikkeling van een platform voor het delen van fraudegegevens essentieel, waarbij bijkomende

fraude-indicatoren dienen te worden geïntegreerd, zoals signalen afkomstig van het mobiele toestel van het slachtoffer.

Op korte termijn zal het platform gericht zijn op het delen van gegevens over geldezels. Op middellange en lange termijn is het de ambitie om de scope uit te breiden met signalen uit meerdere bronnen, zoals telecomgegevens, toestelgegevens en itsme®.

Dit initiatief sluit aan bij de nationale prioriteiten en bij de richting van het toekomstige Europese regelgevend kader, dat steeds meer belang hecht aan het delen van fraudegerelateerde informatie in de strijd tegen online fraude. Dergelijke initiatieven vereisen **rechtszekerheid** en een passend kader, zodat gegevensuitwisseling veilig, proportioneel en conform de regelgeving kan gebeuren. Politieke steun en de actieve betrokkenheid van toezichthouders (waaronder de Gegevensbeschermings-autoriteit) zijn daarom essentieel om een doeltreffende samenwerking mogelijk te maken en te vermijden dat criminelen misbruik kunnen maken van lacunes. In dit verband blijft het cruciaal dat banken een bestaande of nieuwe klantenrelatie met de geïdentificeerde fraudeur(s) kunnen beoordelen in overeenstemming met de toepasselijke wetgeving, waaronder de regels inzake AML en PAD.

Banken pleiten al jaren voor de mogelijkheid om fraudegegevens beter te delen. Vandaag kunnen enkel banken die rechtstreeks betrokken zijn bij een fraudegeval bilateraal informatie uitwisselen, bijvoorbeeld over geldezels. Die informatie mag niet met een andere bank worden gedeeld, waardoor het veel moeilijker is om fraudeurs en geldezels echt tegen te houden. Dankzij samenwerking kunnen we een nog efficiëntere strijd tegen fraude voeren.

Beoogde timing: pilootfase Q1 2027

5. **Communicatiecharter – engagement van de banksector om fraudedossiers binnen 15 bankwerkdagen te behandelen**

Een andere prioriteit is **de harmonisering van de communicatie met klanten en de behandeling van fraudedossiers**. De sector engageert zich om fraudedossiers binnen maximaal **15 bankwerkdagen** te behandelen[2]. Dat engagement zal worden ondersteund door specifieke procedures voor de behandeling van fraudedossiers, gestandaardiseerde verwerkingstermijnen en de integratie ervan in een communicatiecharter voor de hele sector. Deze maatregel sluit eveneens aan bij het toekomstige PSR-kader.

Het communicatiecharter heeft als doel een duidelijke en consistente klantervaring te waarborgen. Daarbij staan enkele principes centraal: snel handelen, 24/7 bereikbaar zijn, de klant meteen beschermen, hem of haar goed informeren en stap voor stap begeleiden, werken met één centraal dossier, samenwerken met de politie en dezelfde ondersteuning bieden ongeacht het kanaal waarlangs de fraude wordt gemeld. Met dit charter verbinden banken zich ertoe klanten die

[2] Indien bij een fraudegeval buitenlandse banken betrokken zijn, kan deze termijn van 15 dagen evenwel worden overschreden.

slachtoffer zijn geworden van online fraude de juiste informatie en de nodige begeleiding te bieden, met aandacht voor hun individueel dossier. **Beoogde timing: Q4 2026**

Febelfin actieplan niveau 3 – Samenwerking binnen het hele ecosysteem

Het is belangrijk om te benadrukken dat maatregelen van banken alleen — zowel op individueel niveau als op sectorniveau — niet volstaan om blijvende resultaten te boeken. Zonder een **volwaardige samenwerking binnen het hele ecosysteem** en zonder doeltreffende maatregelen van andere publieke en private stakeholders, zowel aan **het begin als aan het einde van de fraudeketen**, dreigen bijkomende maatregelen van banken vooral de gevolgen van fraude te beperken, zonder de oorzaken ervan structureel aan te pakken. We verwijzen daarbij naar voorbeelden uit het Verenigd Koninkrijk en Nederland.

Een gecoördineerde aanpak binnen het hele ecosysteem is bovendien cruciaal om te vermijden dat er verschillen ontstaan in regelgeving of in de manier waarop fraude wordt aangepakt. Zo'n verschillen zouden België aantrekkelijker kunnen maken voor fraudeurs. Als fraude niet overal in de fraudeketen of niet in alle landen op dezelfde manier wordt aangepakt, bestaat dus het risico dat criminele activiteiten zich richten op de zwakste schakel. Banken zijn bereid hun eigen maatregelen verder te versterken, maar dat kan alleen doeltreffend zijn als alle publieke en private stakeholders aanvullende maatregelen nemen om fraude in elke fase aan te pakken.

Febelfin vraagt de overheid om de volgende maatregelen te nemen:

1. **De rol van het CCB als centrale coördinator versterken**
2. **Telecombedrijven en sociale media platformen een grotere rol laten opnemen**
3. **De wetshandhaving versterken (politie en justitie)**
4. **Sterke klantauthenticatie (SCA) bij online transacties versterken ('soft decline')**
5. **De overheid als facilitator: het wettelijk kader aanpassen waar nodig**
6. **Afstemming op Europees niveau en vermijden van versnippering en gold plating**
7. **Gezamenlijke sensibiliseringscampagnes ondersteunen**

1. De rol van het CCB als centrale coördinator versterken

Febelfin pleit voor een gecoördineerde aanpak binnen het volledige ecosysteem, waarbij de overheid een coördinerende rol op zich neemt en waarbij alle relevante publieke en private stakeholders worden betrokken. Het Centrum voor Cybersecurity België (CCB) is de bevoegde instantie op het vlak van cyberveiligheid. Om deze aanpak doeltreffend te maken, moeten twee prioriteiten worden nagestreefd:

- De **ontwikkeling van een nationaal antifraudeplan**, waaraan de banken actief zullen bijdragen. Zo'n plan is nodig om prioriteiten op elkaar af te stemmen, versnippering te vermijden en ervoor te zorgen dat preventie, detectie, melding, onderzoek en handhaving op een coherente manier worden aangepakt.

- De rol van het CCB als centrale coördinator moet worden versterkt. Dat kan door het CCB een gecentraliseerd coördinatieplatform te laten voorzitten dat alle relevante publieke en private stakeholders samenbrengt, de uitvoering van het nationale antifraudeplan aanstuurt en een doeltreffende samenwerking waarborgt.

2. Telecombedrijven en sociale media platformen moeten een grotere rol opnemen

Telecomoperatoren en sociale media platformen spelen een c**ruciale rol in de eerste fases van online fraude en moeten een grotere rol opnemen**. Fraudeurs gebruiken vaak telecomkanalen voor hun oproepen en berichten, terwijl ze sociale media en advertentieplatformen inzetten om advertenties te verspreiden, zich voor te doen als betrouwbare partijen en geldezels te ronselen. Dit zorgt ervoor dat zij belangrijke signalen van fraude al in een vroeg stadium kunnen opsporen en zo fraude tegenhouden. Hun verantwoordelijkheden moeten daarom duidelijker worden vastgelegd en uitgebreid, vanuit het principe dat alle betrokken spelers een gedeelde verantwoordelijkheid dragen.

Voor sociale media platformen en Big Tech betekent dit onder meer een snellere detectie en het verwijderen van frauduleuze advertenties, accounts en inhoud, en duidelijke aansprakelijkheid in lijn met de Digital Services Act en het toekomstige PSR-kader. Ook moet worden onderzocht wie binnen dit kader als 'trusted flagger' kan optreden om frauduleuze advertenties te melden.

Daarnaast moet de samenwerking tussen sociale media platformen, telecomoperatoren en banken worden versterkt, onder meer door mechanismen te ontwikkelen om relevante fraudegerelateerde informatie te delen in lijn met het toekomstige PSR-kader. In deze context kunnen bijkomende wetgevende initiatieven of verduidelijkingen nodig zijn om een solide juridische basis te creëren, rechtszekerheid te bieden en tegelijk de regelgeving inzake gegevensbescherming te respecteren.

Telecomoperatoren kunnen hierbij een sleutelrol spelen door systemen te ontwikkelen om gegevens te delen met banken en itsme®, zodat belangrijke signalen zoals recente simkaartwissels (SIM-swap), lijnbezetting, verdachte nummers of bepaalde communicatiemetadata kunnen worden uitgewisseld. Het delen van deze informatie moet binnen een duidelijk, proportioneel en juridisch robuust kader gebeuren. Betere samenwerking maakt het mogelijk om fraude sneller op te sporen tijdens transacties en geeft een duidelijker beeld van de volledige fraudeketen.

Er is nood aan **strenger toezicht op en strengere vereisten** voor telecomoperatoren en sociale media platformen, zodat zij hun verplichtingen ook effectief naleven:

- Het is bijvoorbeeld moeilijk te begrijpen dat iemand erin slaagt honderden simkaarten aan te kopen met de identiteitskaart van een familielid. Dergelijke feiten kunnen wijzen op fraude en moeten daarom kordaat worden aangepakt door telecomoperatoren, in lijn met de verplichtingen rond eindgebruikersidentificatie die de Belgische wet oplegt.
- Ook het huidige port-outproces roept vragen op. Bij sommige operatoren kan een fraudeur het telefoonnummer van iemand anders overnemen op basis van enkel het klantnummer dat aan het telecomaccount is gekoppeld — informatie die via phishing relatief makkelijk kan worden

verkregen. Vervolgens kan de fraudeur een simswap aanvragen en een nieuwe simkaart laten leveren op een adres naar keuze. Zulke tekortkomingen tonen aan dat strenger toezicht en sterkere controles nodig zijn. Ze maken fraude niet alleen makkelijker, maar roepen ook ernstige vragen op over KYC en klantenidentificatie.

- Uit rapporten blijkt bovendien dat frauduleuze advertenties voor sociale mediaplatformen een verdienmodel zijn[3]. Deze platformen moeten frauduleuze websites offline halen, in lijn met de Europese Digital Services Act.

3. De wetshandhaving versterken (politie en justitie)

Banken pleiten ook voor een nauwere samenwerking met politie en justitie, aangezien zij een cruciale rol spelen aan het einde van de fraudeketen. Banken kunnen fraude voorkomen, detecteren, transacties blokkeren en gestolen geld proberen recupereren, maar alleen politie en justitie kunnen **onderzoek doen naar criminele netwerken, daders vervolgen en georganiseerde misdaad bestrijden**. Dat is essentieel, want fraude wordt steeds vaker georganiseerd, grensoverschrijdend en op grote schaal gepleegd. Daarbij wordt geld vaak via geldezels, meerdere banken, cryptoactiva of buitenlandse jurisdicties doorgesluisd.

Febelfin vraagt daarom om een **sterkere nationale coördinatie** met politie, parket en rechtbanken. Die moet gepaard gaan met voldoende middelen, gespecialiseerde expertise en een snellere uitwisseling van informatie tussen banken en ordediensten. De samenwerking moet verder gaan dan een aanpak per individueel dossier en evolueren naar een meer strategische aanpak, gericht op het herkennen van patronen, het traceren van geldstromen en het aanpakken van de criminele organisaties achter fraude.

Een pilootproject met het parket kan bijvoorbeeld de samenwerking concreet vormgeven en de aanpak verschuiven van het behandelen van afzonderlijke dossiers naar het ontmantelen van georganiseerde fraudenetwerken. De politie en het openbaar ministerie moeten toegang krijgen tot het (toekomstige) platform voor het delen van fraudegegevens en er ook zelf gegevens aan kunnen toevoegen. Een sterkere inzet van politie en justitie is essentieel als aanvulling op de preventieve maatregelen van banken, om ervoor te zorgen dat we in de strijd tegen online fraude niet alleen slachtoffers beschermen, maar ook de criminele bron aanpakken.

Febelfin benadrukt dat de overheid de nodige middelen moet investeren in politie en justitie. Een gebrek aan middelen en een te beperkte vervolging leiden tot straffeloosheid en maken ons land aantrekkelijker voor fraudeurs. Dat moet worden vermeden, zowel om criminelen af te schrikken als om het gevoel van straffeloosheid bij slachtoffers te verminderen.

[3] https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

4. **Sterke klantauthenticatie (SCA) bij online transacties optimaliseren (‘soft decline’)**

Banken zullen het initiatief nemen om **sterke klantauthenticatie verplicht te maken voor bepaalde online transacties**, via een sectorbrede overeenkomst en/of een verzoek aan de toezichthouder, met name voor transacties waarbij geen fysieke bankkaart wordt gebruikt (card-not-present of CNP), naar het voorbeeld van de Franse maatregel.

De PSD2-richtlijn voorziet uitzonderingen op het gebruik van sterke klantauthenticatie bij online transacties. Zo is SCA bijvoorbeeld niet vereist bij een gekende begunstigde of bij kleine bedragen met een beperkt risico. Net die uitzonderingen kunnen in bepaalde gevallen leiden tot fraude, meestal voor relatief beperkte bedragen. Door het mechanisme van ‘soft decline’ toe te passen — waarbij een betalingsverzoek zonder SCA wordt geweigerd, maar de handelaar het betalingsverzoek opnieuw kan indienen mét SCA — kan dit probleem grotendeels worden aangepakt.

5. **De overheid als facilitator: het wettelijk kader aanpassen waar nodig**

Sommige bancaire maatregelen kunnen alleen worden uitgevoerd als **bepaalde wetgeving** binnen een redelijke termijn wordt gehandhaafd en/of aangepast:

- Het delen van fraudegegevens: uitwisseling van gegevens over geldezels tussen banken, zoals naam en rijksregisternummer.
- De uitwisseling van telecom metadata (bv. of er een gesprek bezig is, de duur van het gesprek, enz.)
- Het gebruik van biometrische gegevens bij gedragsgebaseerde transactiemonitoring, bijvoorbeeld via individuele profilering in het kader van fraudedetectie.
- Sociale media platformen moeten frauduleuze advertenties sneller offline halen en juridisch aansprakelijk kunnen worden gesteld, in overeenstemming met de Europese Digital Services Act (DSA) en de PSR.
- Er moet worden onderzocht wie binnen dit wettelijk kader als ‘trusted flagger’ kan worden aangeduid om betrouwbare meldingen van frauduleuze advertenties in te dienen.
- Telecomoperatoren moeten de verplichtingen inzake eindgebruikersidentificatie naleven die door de Belgische wet worden opgelegd.

6. **Afstemming op Europees niveau en vermijden van versnippering en goldplating**

Deze drieledige aanpak heeft tot doel de bescherming van klanten te versterken en tegelijk in **overeenstemming te blijven met het Europese regelgevingskader** dat in ontwikkeling is. De sector benadrukt het belang van afstemming op Europese regels en de noodzaak om nationale gold plating of versnipperde initiatieven te vermijden, omdat die de rechtszekerheid en operationele doeltreffendheid kunnen ondermijnen.

7. Gezamenlijke sensibiliseringscampagnes ondersteunen

Sensibiliseringscampagnes zijn een essentieel onderdeel van **fraudepreventie**. De banksector engageert zich tot een gezamenlijke communicatieaanpak en zal een campagne ontwikkelen die fraude blijvend onder de aandacht brengt van het brede publiek en klanten aanmoedigt om concrete, bewuste keuzes te maken die hun blootstelling aan fraude verminderen. De sector zal hierin blijven investeren om consumenten weerbaarder te maken en fraude zo veel mogelijk te voorkomen. Het is belangrijk dat zowel de overheid als andere stakeholders deze campagnes ondersteunen en faciliteren, naar analogie met de BOB-campagnes. Een dergelijke gecoördineerde aanpak kan een sterk hefboomeffect creëren, fraudepreventie verder versterken en de weerbaarheid van burgers vergroten.

Conclusie

Online fraude is vandaag een structurele maatschappelijke uitdaging die voortdurend evolueert en niet langer kan worden aangepakt met afzonderlijke maatregelen of door één groep stakeholders alleen. **De banksector neemt ten volle zijn verantwoordelijkheid en heeft al verregaande initiatieven genomen om klanten beter te beschermen, fraudedetectie te verbeteren en slachtoffers te ondersteunen. Dit zullen we in de toekomst ook blijven doen.** Met dit actieplan verbinden banken zich ertoe hun inspanningen verder uit te breiden, zowel op individueel als op sectorniveau, onder meer via bijkomende operationele maatregelen, sterkere samenwerking en meer sensibilisering van consumenten.

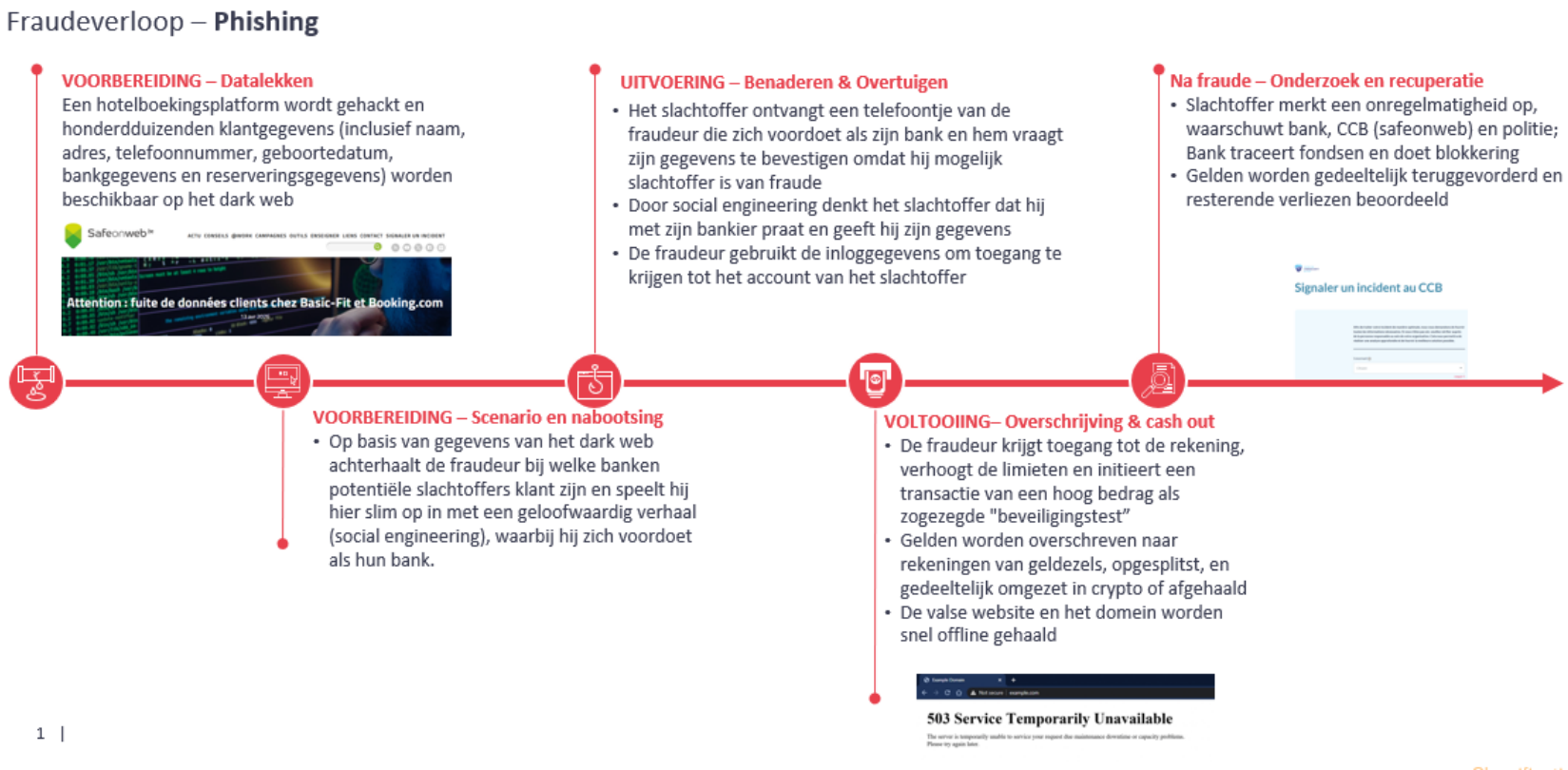
Tegelijk toont dit actieplan duidelijk aan dat bancaire maatregelen alleen niet volstaan om online fraude duurzaam terug te dringen. Zelfs de meest robuuste maatregelen op bankniveau en tussen banken onderling zullen slechts een deel van het probleem kunnen aanpakken zolang fraude elders in de keten ontstaat en verder evolueert. **Een blijvende impact vereist een volledig gecoördineerde aanpak binnen het hele ecosysteem, waarin alle relevante publieke en private stakeholders hun verantwoordelijkheid opnemen** en op een coherente en complementaire manier samenwerken.

Banken zijn bereid om hun initiatieven uit te breiden en te blijven investeren in preventie, detectie en klantenbescherming. Die inspanningen kunnen echter alleen doeltreffend zijn als ze gepaard gaan met daadkrachtige acties aan het begin en aan het einde van de fraudeketen, onder meer door online platformen, telecomoperatoren, politie, justitie en overheidsinstanties. Zonder die samenwerking dreigt fraude zich eenvoudigweg te verplaatsen naar de zwakste schakel in de keten. **Net daarom is een gecoördineerde aanpak nodig om te vermijden dat België een aantrekkelijk doelwit wordt voor georganiseerde online fraude.**

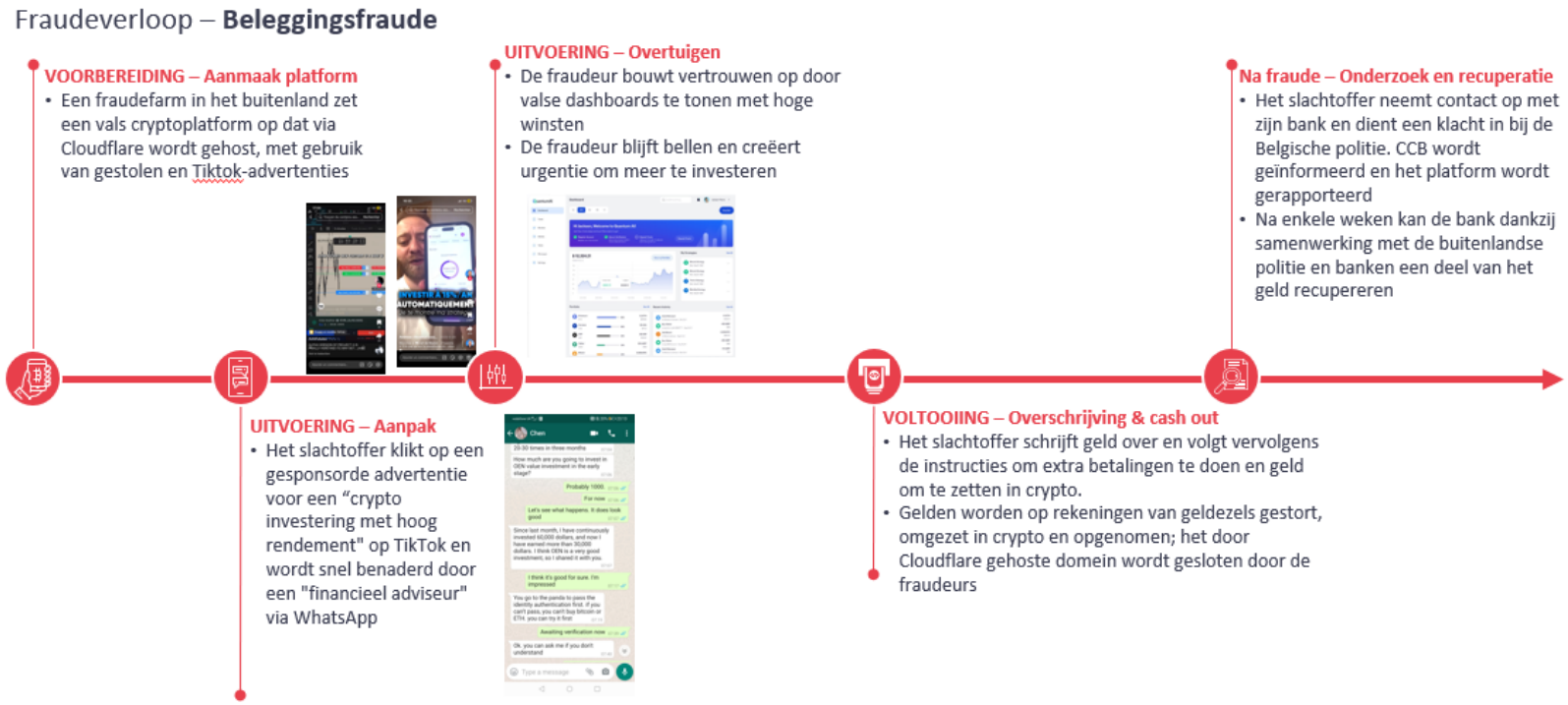
Dit actieplan pleit daarom voor sterke politieke steun, duidelijke coördinatie en een ondersteunend wettelijk kader dat innovatie, gegevensdeling en doeltreffende handhaving mogelijk maakt, binnen een kader dat de fundamentele rechten beschermt. Alleen via een gezamenlijke, evenwichtige en geïntegreerde aanpak kunnen we online fraude bij de bron aanpakken, de bescherming van klanten duurzaam versterken en het vertrouwen in het digitale financiële ecosysteem behouden.

Bijlage: voorbeeld van fraudeverloop

Banken zijn doorgaans pas in een latere fase betrokken — tijdens en na de transactie — terwijl phishing vaak al start via sociale media en valse websites.



Bij beleggingsfraude worden sociale media en telecomkanalen vaak gebruikt om slachtoffers te benaderen en te beïnvloeden, terwijl banken pas betrokken zijn wanneer de transactie plaatsvindt.[45]



[4] "Dans la jungle des néobanques: Arnaques, trafics et clients lésés" – Arte
[5] Krantenknipsel BBC