BW
BANK|WERELD

EXPERTS

van binnen en buiten de financiële sector aan het woord over veiligheid

Nederlandse Vereniging van Banken

VERDER IN DEZE EDITIE

- ***Rondetafelgesprek*** *Samen muren bouwen tegen crimineel geld*
- ***Publiek-private samenwerking*** *legt stevig fundament in voorkomen en bestrijden witwassen*
- ***Strijd tegen plofkraak-crimineel vergt maat-werk***

VOORJAAR 2020
Veiligheid

CRIMINALITEIT, OOK IN CORONATIJD

Alsof we onze handen niet vol hebben in Nederland aan het bestrijden van de coronacrisis, spelen sluwe criminelen hierop in. Al vroeg tijdens de coronacrisis zagen wij ons als bankensector genoodzaakt een tv-spot te maken om mensen te waarschuwen tegen cybercriminelen die zich met gladde verhalen melden op jouw smartphone of vaste computer. Zogenaamd als jouw bank die je vertelt dat je een anti-bacteriële betaalpas moet hebben. Of als jouw baas met het dringende verzoek een groot bedrag over te maken voor de aanschaf van een grote partij handgel en mondkapjes.

Criminelen ondermijnen onze samenleving. Dat gaat van fraude met betaalpassen tot grootscheepse grensoverschrijdende witwasoperaties. Overheidsinstanties en veel mensen kijken naar banken als het gaat om het ontdekken en tegengaan hiervan. Banken investeren op grote schaal in het screenen van hun klanten en het monitoren van betaaltransacties en melden ongebruikelijke zaken aan de autoriteiten. In Nederland zijn op moment naar schatting ruim 8.000 bankmedewerkers fulltime ingeschakeld bij de strijd tegen het witwassen.

Banken kunnen veel zien in hun systemen, maar niet alles. Daarom is onderlinge en publiek-private samenwerking waarbij 'intelligence' kan worden uitgewisseld van groot belang. Onderling onderzoeken vijf banken samen met de Nederlandse Vereniging van Banken de mogelijkheid tot oprichting van een gezamenlijke organisatie, Transactie Monitoring Nederland, zodat patronen sneller worden herkend. En samen met de publieke partijen die zijn verenigd in het Financieel Expertise Centrum speuren banken niet alleen naar aanwijzingen voor witwassen maar ook voor mensenhandel en terrorismefinanciering.

Niet alleen proberen we in deze tijd met elkaar onze samenleving gezond te houden en onze economie te redden, ook werken we hard aan het waarborgen van onze veiligheid en de integriteit van ons financiële systeem. Over de uiteenlopende initiateven van banken en hun maatschappelijke partners op het gebied van veiligheid gaat dit themanummer van Bank|Wereld.

Gezondheid, voorspoed en veiligheid zijn onlosmakelijk met elkaar verbonden. Banken dragen hier graag aan bij, in het belang van hun klanten en de samenleving.

Chris Buijink
Voorzitter Nederlandse Vereniging van Banken

COLOFON

Redactieadres
Gustav Mahlerplein 29-35,
1082 MS Amsterdam
Postbus 7400,
1007 JK Amsterdam
020 550 2888
info@nvb.nl

Eindredactie
Hanan Laghmouchi,
Bart van Leeuwen

Redactie
Mireille Reijs, Maurits de Nerée tot Babberich, Paul van Kempen, Ivo Bolluijt, Geert Gladdines, Jelle Wijkstra, Mark van Limburg, Agnieta van der Plaat, Robert Jan Prins, Yvonne Willemsen, Hans van Loon, Puck van der Laan, Jeroen Rijpkema, Jeroen Buunen

Fotografie
Evelien Hogers Fotografie, Marcel Molle, beeldbank EBF, coverfoto: www.janekoenig.com

Vormgeving
Yardmen bv, Amsterdam

BW
BANK|WERELD

inhoud

2 ***Chris Buijink***
Voorwoord van de voorzitter

4 ***Cyberveiligheid in een digitale wereld***
Wilma van Dijk (Schiphol)

8 ***Publiek-private samenwerking legt stevig fundament in voorkomen en bestrijden witwassen***
Nieke Martens (Rabobank), Jeroen Toor (FIU-Nederland), Iris Sluiter (FEC), Jaap Piersma (Politie) en Martijn Koch (FIOD)

12 ***Samen muren bouwen tegen crimineel geld***
Robin de Jongh (ABN AMRO), Jane Lobbrecht (Triodos) en Jeroen Rijpkema (Nederlandse Vereniging van Banken)

16 ***Alleen Europese witwasaaanpak kan tij keren***
Wim Mijs (European Banking Federation)

18 ***Veilig financieel ouder worden begint lokaal***
Marianne van der Krans (Veilig Thuis), Roxana Faujdar (Rabobank) en Jasper Grotjohann (ABN AMRO)

21 ***Gastcolumn***
Wim Hafkamp (Z-CERT)

22 ***Strijd tegen plofkraakcrimineel vergt maatwerk***
Peggy Corstens (Geldmaat) en Job Galesloot (ING)

25 ***Profiel van een bankmedewerker***
Leonie Bik (De Volksbank)

26 ***Fraude in het betalingsverkeer"***
Laurine van Teulingen (ABN AMRO)

28 ***Corona Monitor***

Nederlandse Vereniging van Banken

VOORJAAR 2020
Veiligheid

CYBER VEILIGHEID IN EEN DIGITALE WERELD

IN GESPREK MET WILMA VAN DIJK, DIRECTEUR SAFETY, SECURITY & ENVIRONMENT BIJ SCHIPHOL

BW
BANK|WERELD

Veiligheid in al zijn facetten staat op luchthaven Schiphol natuurlijk op nummer één. Spil daarin is Wilma van Dijk, directeur Safety, Security & Environment bij Schiphol. Ook is Van Dijk voorzitter van de Commissie Vitale Infrastructuur (CVI) van VNO NCW, en op dit moment zit haar termijn van vier jaar er bijna op. Goed moment voor de brede visie van Van Dijk op een cyberveilig Nederland.

"De CVI behartigt de sector-overstijgende belangen van de private vitale sectoren en bedrijven inzake nationale veiligheid en vitale infrastructuur. Ook formuleert de CVI het VNO-NCW beleid hierin", zo omschrijft Van Dijk de commissie waarvan ze binnenkort afscheid neemt.
"We vormen een netwerk voor intersectorale uitwisseling van kennis, informatie, ervaringen en best practices. We volgen kritisch het relevante overheidsbeleid en (inter)nationale wet- en regelgeving en spreken ons hierover uit. Ook fungeren we als klankbord voor de overheid. In de huidige coronacrisis zijn we onder meer ook klankbord en 'doorgeefluik' van informatie. Een centrale 'hub' voor informatiedeling tussen de vitale aanbieders. We behartigen hun belangen en zijn een linking pin met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Dat leidde onder meer tot de 'Verklaring van vitaal belang'."

NIET OVERAL EVEN HOOG OP DE AGENDA

Voor haar rol als directeur bij Schiphol was Van Dijk ruim vier jaar directeur Cybersecurity bij de NCTV. Op de vraag of Nederland cyberveilig is en waar de sterke punten en verbeterpunten liggen, antwoord Van Dijk: "Nederland heeft een sterke cultuur van vrijwillige samenwerking en kennisdelen voor een gedeeld resultaat. De afgelopen tien jaar zijn veel goede stappen gezet in publiek-private samenwerking en kennisdeling voor een cyberveilig Nederland. De vitale sectoren nemen allerlei extra maatregelen. Dit in nauwe samenwerking met de vakdepartementen en toezichthouders. Maar cybersecurity staat niet bij alle Nederlandse – publieke en private – organisaties even hoog op de agenda. Hier is zeker verbetering en versnelling mogelijk. Ook valt er winst behalen door samen te oefenen en leren."

ROL OVERHEID CYBERVEILIG NL

Van Dijk: "In mijn ogen is de rol van de overheid het ondersteunen en adviseren van vitale bedrijven, en in het bijzonder het delen van betrouwbare informatie over dreigingen - met bijbehorend handelingsperspectief. Dan kunnen bedrijven maatregelen treffen en investeren in preventie. Ook zou de overheid een regierol kunnen pakken bij de realisatie van één loket, waar bedrijven terechtkunnen voor informatie en vragen over cyberveiligheid. Juist bij bedrijven in de vitale infrastructuur, waaronder Schiphol, staat cybersecurity zeer hoog op de agenda. Samen en in nauw overleg met vakdepartementen en toezichthouders zijn ze volop bezig met de invulling van hun wettelijke zorgplicht. Belangrijk om hierbij op te merken, is dat honderd procent veiligheid niet bestaat. Cyberincidenten zullen er altijd zijn."
"En over een meer sturende rol voor de overheid: ik onderschrijf het achterliggende doel dat cybersecurity alle aandacht verdient. Cybersecurity is randvoorwaardelijk voor digitalisering én voor de nationale veiligheid. Wel is er al een zeer uitgebreid stelsel van sectorale toezichthouders. Een extra autoriteit – dus een nieuwe toezichtslaag – lijkt mij niet nodig. Het zou zelfs afbreuk kunnen doen aan de publiek-private samenwerking die onder meer is gebaseerd op vertrouwen, kennisuitwisseling en leren van incidenten in een open cultuur. Binnen de luchtvaart geldt al heel lang dat het meest wordt geleerd van vooral veel kleine dingen die fout gaan. En dat je door het open delen van kennis hierover, grotere incidenten tijdig kunt voorkomen. Een actieve meldingscultuur is onontbeerlijk. Zit de toezichthouder aan tafel als incidenten worden besproken, dan is de kans groot dat er minder gemeld wordt en dat het lerend vermogen drastisch afneemt."

PERMANENTE AANDACHT

De samenleving wordt toenemend digitaal afhankelijk, ziet ook van Dijk: "Digitale infrastructuur is inmiddels volledig verweven met processen die cruciaal zijn voor de samenleving, de economie en de democratische rechtstaat. Voor veel processen bestaat geen analoog alternatief meer. De aandacht voor digitale continuïteit en het voorkomen van digitale ontwrichting is echter nog niet overal even groot. Permanente aandacht voor het zo klein mogelijk houden van cyberrisico's is onlosmakelijk verbonden met de verdergaande digitalisering. Dit vraagt om een proactieve en bewuste houding van overheid, bedrijfs-

>>

leven en burgers. En om een proactieve publiek-private samenwerking waarin preventie, kennisdeling en van elkaar leren centraal staan."

Nederland moet zich beschermen tegen cybercriminelen die vaak ook grensoverschrijdend werken. Van Dijk: "Los van onze eigen verantwoordelijkheid als bedrijfsleven, zijn we hierin echt afhankelijk van de informatie die de overheid ons geeft. Informatiedeling over cyberdreigingen, zeker over statelijke actoren, is noodzakelijk om de cyberveiligheid op niveau te kunnen houden en te versterken. Juridische obstakels die informatiedeling belemmeren, zouden moeten worden geslecht. Voorwaarde is dan natuurlijk dat de overheid de juiste specialisatie in huis heeft om dit goed te doen. Ook bepleit de CVI een versteviging van de internationale samenwerking."

DIGITALE ONTWRICHTING

Op de vraag voor welke opgave Nederland staat bij het digitaal veilig houden van vitale diensten als watervoorziening, telecom, elektriciteit en ook bankdiensten, antwoordt Van Dijk: "Opgave is om cybersecurity altijd hoog op de agenda te houden. Proactieve publiek-private kennisdeling blijft nodig voor de juiste preventie-investeringen."

In 2019 pleitte de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) voor een betere voorbereiding op een digitale ontwrichting; onder meer middels adequate bevoegdheden om escalatie te voorkomen en inspanningen op cyberverzekeringen. Van Dijk onderschrijft het belang van voorbereiding: "De CVI benadrukt al langer het belang van een structurele, gezamenlijke oefenagenda. Samen scenario's oefenen geeft inzicht in de gezamenlijke doelen en welke ondersteunende processen en technieken belangrijk zijn. Ook wordt de weerbaarheid van het geheel getoetst. Belangrijke verbeteringen komen zo aan het licht. Net zo relevant – en vaak onderbelicht – zijn een goede evaluatie van bestaande incidenten en een follow up."

"Bij calamiteiten is het natuurlijk extra belangrijk dat vitale diensten beschikbaar blijven, vervolgt Van Dijk. "Naast de interactie georganiseerd op basis van calamiteitenplannen is er ook extra afstemming en informatie-uitwisseling. Het gemeenschappelijk maatschappelijk belang staat voorop. En als het gaat om financiële instellingen: die worden het meest van alle sectoren aangevallen. Door de snelle digitalisering groeit hun aanvalsoppervlak. Dat risico hebben financiële instellingen in het algemeen al lang geleden onderkend. Hun cyber resilience is dus ook navenant. Wat ik krachtig blijf vinden in de financiële sector, is de open samenwerking op cyber security. Bij Schiphol hebben we daar veelvuldig baat bij gehad, in contacten met meerdere banken. Ik denk dat veel financiële instellingen al een belangrijke maatschappelijke bijdrage leveren door het delen van hun kennis en ervaring en significant te investeren in cyber security."

WIN/WIN-SITUATIE

Een nauwe publiek-private samenwerking is dé sleutel bij het digitaal veilig houden van de vitale diensten, benadrukt Van Dijk: "Schiphol heeft ervaren dat daarmee veel winst te behalen is, als partijen uitgaan van vertrouwen, elkaars rol en verantwoordelijkheden erkennen, kennis delen en gezamenlijk veiligheidsprojecten uitvoeren. Bedrijven staan hiervoor open; een win/win-situatie. Binnen het NCSC wordt intensief publiek-privaat samengewerkt. De overheid speelt hier een belangrijke rol in. De betrokken overheidsinstanties moeten dan wel beschikken over de juiste (IT en OT) kennis en expertise. De CVI pleit daarom voor investeringen in meer kennis en expertise bij de overheid waar nodig."
"Voor de vitale infrastructuur is er een goed werkend stelsel van toezicht en handhaving, belegd bij de sectorale toezichthouders (AT, DNB en ILT). Daarnaast kan het ministerie van Justitie en Veiligheid escaleren naar vakdepartementen en toezichthouders als men vindt dat vitale bedrijven onvoldoende gehoor geven aan de adviezen. Toezichthouders kunnen op hun beurt eventueel de betrokken bedrijven aanwijzingen geven, dan wel maatregelen afdwingen. Het toezicht is zo in mijn ogen voldoende en adequaat ingericht."

LESSONS LEARNED IN CORONACRISIS?

Op de vraag of er al 'lessons learned' zijn inzake de continuïteit van de vitale sectoren in deze coronacrisis, antwoordt Van Dijk: "Veel issues komen nu scherper naar voren. Zo ook de noodzaak tot digitale veiligheid, in deze tijd van versnelde digitale afhankelijkheid. Het proactief signaleren en oplossen van cyberkwetsbaarheden is essentieel. Daartoe moeten alle bedrijven en organisaties toegang krijgen tot relevante (operationele) cyberinformatie. En voor de vitale sectoren zijn trusted channels nodig, voor het delen van geclassificeerde informatie. Ook zouden we - in publiek-privaat samenwerkingsverband - meer inzicht moeten verkrijgen in de ketenafhankelijkheden in de kritische ICT-processen, om beter te kunnen sturen op de continuïteit van de vitale ICT-ketens. En, nogmaals, we moeten ook nu van elkaar leren door te oefenen." —

Als directeur Safety, Security & Environment bij **Schiphol** is **Wilma van Dijk** verantwoordelijk voor het beleid en de uitvoering op aviation security, access control, cybersecurity (CISO van Schiphol) en company security. Dit bevat meer de dagelijkse 24-uurs security-operatie, contractbeheer, contacten met (inter)nationale overheidsinstanties, particuliere beveiligingsbedrijven en technische ontwikkelingsbedrijven. Ook is Van Dijk verantwoordelijk voor het beleid in Safety & Environment op de luchthaven, en voor de luchthavenbrandweer. Verder is Van Dijk verantwoordelijk voor Seamless Flow, het innovatieve programma dat middels biometrie moet zorgen voor een veilige, zorgeloze en papierloze passage op de luchthaven. Verder is Van Dijk vanaf 1 juni ook algemeen directeur van Lelystad Airport.

PUBLIEK-PRIVATE SAMENWERKING LEGT STEVIG FUNDAMENT IN **VOORKOMEN EN BESTRIJDEN WITWASSEN**

De banken en publieke partijen hebben afspraken gemaakt om nog effectiever samen te werken in de strijd tegen witwassen. Een gesprek met de vijf kwartiermakers over 'de heilige graal' van het delen van kennis

Een pizzeria waarvan de omzet niet inzakt in coronatijd. Is dat ongebruikelijk? Om die vraag te beantwoorden, zegt Nieke Martens, Global Head Future KYC bij Rabobank, is de kennis nodig van zowel de banken als de opsporingsinstanties. "De eerste zien alle transacties en de opsporingsinstanties hebben kennis van criminele fenomenen. Door die twee bij elkaar te brengen, kun je medewerkers van de banken meegeven: ja, dit kan ongebruikelijk zijn."

Overheidspartijen en banken weten elkaar al langer te vinden als het gaat om bestrijding van witwassen, onder meer binnen het Financieel Expertise Centrum (FEC). De zeven partners van het FEC (Autoriteit Financiële Markten, Belastingdienst, De Nederlandsche Bank, Financial Intelligence Unit-Nederland, FIOD, Openbaar Ministerie en Politie) werken op verschillende thema's samen met de banken. Nieuwe witwasschandalen in Nederland en elders in Europa brachten deze vorm van financiële criminaliteit vorig jaar opnieuw hoog op de agenda. "Iedereen vond: nu moeten we doorpakken", zo blikt Iris Sluiter van het FEC terug. Ze was na veertien jaar Nederlandsche Bank net begonnen als hoofd van het FEC toen de publieke en private partijen besloten dat er effectiever moest worden samengewerkt. "Er waren goede discussies tussen bestuurders. En het besef dat witwassen alleen teruggedrongen kan worden door samen op te trekken, werd sterker dan ooit gedeeld."

Er werden vijf kwartiermakers naar voren geschoven om de ambities waar te maken. Het doel: 'de banken als poortwachter zo goed mogelijk in staat stellen ongebruikelijke transacties te herkennen en daarop actie te ondernemen. En vervolgens kunnen publieke partijen ook effectiever opsporen en vervolgen.'

Het delen en ontwikkelen van kennis in de keten staat aan de basis van de nieuwe aanpak. Banken hebben de kennis en technologie om met query's te zoeken in grote hoeveelheden data, maar ze moeten wel weten waarnaar ze moeten zoeken. Nieke Martens: "De banken monitoren per uur gezamenlijk 1,3 miljoen transacties. Als je niet weet dat je een blauw strootje in de hooiberg zoekt, vind je het niet. De kennisdeling in de keten is een van de dingen die opsporing effectiever maakt. Ieder voor zich kan zijn bijdrage leveren, maar als je de informatie en kennis bij elkaar legt en op elkaar inspeelt bereik je veel meer."

Het onderzoek richt zich nadrukkelijk op het herkennen van fenomenen in de witwaspraktijk, niet op subjecten. Een voorbeeld is trade based money laundering (TBML), het witwassen van geld via bestaande of op gezette handelsstromen. In FEC-verband wordt een nieuwe verschijningsvorm van TBML in kaart gebracht: crimineel geld dat wordt geïnvesteerd in de autobranche. Met elkaar gericht zoeken in financiële sporen is veel effectiever dan een aanpak per instelling, legt Martens uit. Martijn Koch, sinds bijna vier jaar werkzaam bij de FIOD en coördinator publiek-private samenwerking: "Criminelen worden steeds vindingrijker. Ze werken met vormen die dicht bij de normale bedrijfsvoering passen, zoals bijvoorbeeld spookfacturen. Dat maakt het lastig voor ons om te detecteren. Afzonderlijk kom je er niet achter wat er gebeurt. Dat inzicht krijg je wel door samen te werken in de keten."

Al snel bleek dat er onterechte aannames waren over wat normaal gedrag was in de autobranche, vertelt Koch. "Het idee heerste dat het bij die branche hoort dat er veel cash in omgaat. Query's van de banken maakten echter duidelijk dat die aanname niet klopte. Zelfs zo'n klein inzicht kan iets betekenen. Een bank is dan in staat zijn eigen beleid scherper te stellen: wat valt op en wat is gebruikelijk?"

Nieke Martens vult aan: "Het is belangrijk dat de banken gelijk optrekken. Stel, wij komen erachter dat het gebruik van cash een teken kan zijn van een ongebruikelijke transactie. Als bijvoorbeeld ABN AMRO zijn beleid aanpast en Rabobank niet, dan weten de criminelen dat heel snel. Als de ene bank de deur sluit, gaan de criminelen naar de andere bank. Het is veel krachtiger als alle banken de query draaien en allemaal zeg-

>>

Voorkomen en bestrijden witwassen
Hoofdartikel

gen: dit beleid gaan we veranderen. Je bent veel effectiever als je kennis deelt en samen optrekt. In de toekomst kan Transactie Monitoring Nederland (TMNL)daar een verdere versnelling in aanbrengen als daar query's worden gedraaid op de transacties van de deelnemende banken." In de toekomst worden ook andere sectoren onderzocht op TMBL-constructies. Zo kunnen branche-specifiek witwasindicatoren worden ontwikkeld.

MENSENHANDEL

Een tweede FEC-PPS project dat dit jaar is gestart, betreft witwasstromen in mensenhandel. "Het gaat om menselijke uitbuiting met alle schadelijke gevolgen van dien", onderstreept Jaap Piersma, al 21 jaar werkzaam bij de Politie en sinds vijf jaar betrokken bij de opsporing. "Doelstelling is dan ook tijdiger ingrijpen. Vaak krijgen we pas op een laat tijdstip een melding. Er wordt geld verdiend door iemand uit te buiten. Als we dat eerder traceren en we kunnen die verdachte transacties opwerken tot een strafbare gedraging volgens de wet, kunnen we opsporing inzetten om de mensen te bevrijden en het geldelijk gewin af te pakken." Met dit project borduren de kwartiermakers voort op een zoekprogramma dat eerder is ontwikkeld door de Directie Opsporing van de Inspectie SZW, ABN AMRO en de Universiteit van Amsterdam, in samenwerking met de Financial Intelligence Unit (FIU)-Nederland. Het programma detecteert in bankgegevens signalen van witwassen in verband met sociaaleconomische fraude en mensenhandel. Dat vormt de basis, zegt Jeroen Toor, teamchef binnen FIU-Nederland en verantwoordelijk voor PPS. "Binnen het FEC wordt het nu breder ingezet. De indicatoren worden ingebouwd bij de transactiemonitoring van alle banken. Dat is niet alleen effectiever, maar ook kostenbesparend omdat je ongebruikelijke transacties bijna automatisch gaat herkennen; bijna, want er is altijd nog een menselijke beoordeling nodig voor die conclusie. En omdat de hele keten is aangesloten, komen signalen sneller terecht bij opsporing en kan er uiteindelijk een interventie op worden uitgevoerd."

Samenwerken in de keten moet ook leiden tot kwalitatief betere meldingen en minder false positives. Meldingen van de banken komen binnen bij FIU-Nederland, dat moet onderzoeken of er verdachte transacties bij zijn. In de fenomeengerichte publiek-private samenwerking wordt nu dankbaar gebruik gemaakt van de ervaringen van eerdere projecten tussen de bankensector en onder andere FIU-Nederland: de Terrorisme Financiering Taskforce, de Serious Crime Taskforce en de Fintell Alliance. Medewerkers van FIU-Nederland voorzagen de banken van kennis over het beter en sneller herkennen van witwaspraktijken en leerden op hun beurt van bankmedewerkers over het monitoren van transacties. "Zo krijg je kwalitatief betere meldingen en kun je gemelde transacties effectiever verdacht verklaren", zegt Jeroen Toor van FIU-Nederland. "Wat ons betreft heb je hiermee de heilige graal te pakken."

Focussen op prioriteiten en voortbouwen op successen zijn andere kenmerken van de nieuwe PPS-aanpak. Nieke Martens: "Een issue oppakken, afmaken en dan weer een volgende, in plaats van twintig verschillende initiatieven tegelijk." Focussen op thema's maakt het bovendien makkelijker te communiceren over successen, belangrijk naar de burgers toe, maar ook een signaal voor criminelen. Iris Sluiter van FEC: "Er gaan megabedragen om in witwassen, en dat de praktijken die daaronder schuil gaan ondermijnend werken in de samenleving, wordt ook steeds duidelijker. Maar voor het grote publiek is het onderwerp niet zo tastbaar. Om dat te bereiken moet je problemen concreet benoemen en tonen dat overheid en banken er gezamenlijk werk van maken om die aan te pakken." Het project voor bestrijding van witwasstromen van uitbuitingssituaties is een goed voorbeeld; zo kreeg het beeld van kinderuitbuiting in Australië, pas veel aandacht toen er letterlijk een gezicht van een twaalfjarig meisje bij ging horen.

De kwartiermakers onderstrepen dat deze gezamenlijke aanpak uiteraard altijd plaatsvindt binnen de kaders van de wet, ook als het gaat om privacy. Jeroen Toor: "Banken mogen onderling gegevens delen en de FIU mag daarover adviseren." Query's worden niet gebouwd met criteria als etnische of geloofsachtergrond. "We zien er streng op toe dat er gewerkt volgens de Wet ter voorkoming van witwassen en financieren van terrorisme, de Wwft. Deze samenwerking willen we langdurig en robuust neerzetten. Hij moet goed in elkaar zitten." Elke organisatie blijft verantwoordelijk voor zijn eigen data en heeft daar regie op.

Om de samenwerking tussen publieke en private samenwerking te laten slagen, is het belangrijk naar het gemeenschappelijk doel te blijven kijken, zegt opsporingsambtenaar Jaap Piersma van de Politie. "Er zijn natuurlijk cultuurverschillen. Banken zijn commercieel, bij de politie beschermen we de democratie en handhaven we de openbare orde. Je moet intrinsiek gemotiveerd zijn en de organisatie moet ruimte beschikbaar stellen voor de uitvoering." Verschil in kennis is er ook, beaamt Nieke Martens: "De digitalisering en automatisering zijn bij de banken snel gegaan. Bij banken werken bijvoorbeeld veel datascientists en dat is kennis die goed kan worden ingezet in de keten." Martijn Koch van de FIOD ervaart dat het uiteindelijk mensenwerk is, met korte lijnen tussen de kwartiermakers. Nieke Martens: "Ik zie dat mensen die voor dit werk kiezen enorm gedreven zijn om de wereld beter te maken, die criminaliteit willen bestrijden." Het is tekenend, zegt ze, dat bij de bank op dit thema veel oud-politiemedewerkers werken. "Het is bijna een community." Jaap Piersma waarschuwt vanuit zijn jarenlange beroepspraktijk dat je bereid moet zijn teleurstellingen te incasseren. "Niet stoppen als je een keer vastloopt. Maar doorgaan."

Dat Nederland internationaal voorloopt als het gaat om publiek-private samenwerking in de strijd tegen witwassen, is voor Jeroen Toor een uitgemaakte zaak. "Dat durf ik gerust te zeggen. Ik vind dat het FEC dat meer mag uitstralen." Iris Sluiter knikt. "FEC heeft tot nu toe onder de radar gewerkt, maar dat gaat veranderen. Denemarken, Canada en Zweden hebben veel belangstelling voor onze werkwijze. Canada is ook een soort FEC gestart en kijkt daarbij heel sterk naar Nederland. Uiteindelijk wil je internationaal meer op één lijn komen, zodat je elkaar kunt versterken." Jeroen Toor: "Wat in Nederland ontwikkeld wordt kan vrij gemakkelijk in Europa uitgerold worden. Als alle banken in Europa automatisch dit soort signalen herkennen, ga je een veiligheidsprobleem enorm aanpakken."

Hij omschrijft de samenwerking tussen de banken en de publieke instellingen als "uitermate nuttig". "Ik zie bij banken veel bewustzijn over hun maatschappelijke rol en taak. Ik denk dat we het fundament hebben gelegd, het gebouw heeft een stevige basis, nu moeten er verdiepingen op." —

De vijf kwartiermakers. Van links naar rechts Nieke Martens, Jeroen Toor, Jaap Piersma, Iris Sluiter en Martijn Koch

Gezamenlijk monitoren transacties
RONDETAFELGESPREK

BW
BANK|WERELD

De maatschappelijke ontwrichting en het menselijk leed die gepaard gaan met crimineel geld terugdringen. Dat is de gemeenschappelijk drijfveer van Robin de Jongh (ABN AMRO), Jane Lobbrecht (Triodos) en Jeroen Rijpkema (Nederlandse Vereniging van banken). Samen bouwen ze aan een verdedigingslinie voor de banken. Een gesprek over samenwerking in de strijd tegen witwassen en terrorismefinanciering.

Naar schatting wordt in Nederland jaarlijks zo'n 16 miljard euro witgewassen. Banken en financiële instellingen werken keihard om verdachte transacties in beeld te brengen. In 2018 leidde dat tot 68.000 meldingen van ongebruikelijke transacties bij de FIU. Daarvan werden er 15.000 door de FIU als verdacht aangemerkt.
Ondertussen klinkt overal de roep om meer samenwerking. Nederland loopt hierbij op de troepen vooruit. Binnen Europa wordt er met belangstelling gekeken hoe vijf Nederlandse banken – ABN AMRO, ING, Rabobank, Triodos Bank en de Volksbank – binnen het project Transactie Monitoring Nederland (TMNL) op zoek zijn naar een gezamenlijke aanpak van de strijd tegen witwassen en terrorismefinanciering. Vanuit de Nederlandse Vereniging van Banken (NVB) geeft Jeroen Rijpkema leiding aan dit vooruitstrevende samenwerkingsverband. Robin de Jongh, hoofd detecting financial crime ABN AMRO en Jane Lobbrecht, director operations Triodos Bank zijn vanuit hun banken betrokken.

ENORME IMPACT Alleen al bij deze vijf banken houden zo'n achtduizend medewerkers zich bezig met het opsporen van crimineel geld en dat aantal is alleen maar groeiende. Ze begeven zich op een terrein met een enorme impact op de samenleving. Rijpkema: "Als je praat over witwassen en terrorismefinanciering dan, ligt daaraan altijd menselijk leed ten grondslag. Het is te relateren aan nare zaken als drugs, kinderporno, oplichting of mensenhandel. Geld dat wordt witgewassen wordt vaak weer geïnvesteerd in nieuwe, de maatschappij ontwrichtende criminaliteit."

Zou je kunnen zeggen dat criminelen dankbaar gebruik of zelfs misbruik maken van de fiscale vriendelijkheid van Nederland? "Ik weet het niet", zegt Lobbrecht weifelend. Maar zonder banken wordt iets wat zwart is niet wit; dat is duidelijk." Rijpkema: "Banken en bankmedewerkers die te goeder trouw transacties uitvoeren worden misbruikt. We strijden tegen professionals die proberen de mazen van de wet en de mazen van de verdedigingslinies van de banken op te zoeken. Wat dat betreft zijn Robin en Jane in een zekere *ratrace* verwikkeld tegen het vinden van nieuwe routes en nieuwe manieren."
Het is juist die gehaaidheid van criminelen die het volgens Lobbrecht zo interessant maakt om als banken samen op te trekken. "Criminelen gedijen bij verschil. Door samen te werken voorkomen we dat we tegen elkaar worden uitgespeeld of dat criminelen steeds het laagste gat in de markt vinden."

PASSIE De Jongh wijst erop hoe mooi het is dat banken door hun zicht op financiële transacties een rol kúnnen spelen in de aanpak van crimineel geld en het bestrijden van misstanden.
"We kunnen informatie delen met justitie, waardoor op de lange termijn criminelen kunnen worden opgepakt. Juist omdat het vaak om zulke zware misstanden gaat, zitten we hier met veel passie in. Het maakt dit werk gaaf om te doen."
Lobbrecht herkent dit volledig. "Het bijdragen aan maatschappelijke verantwoordelijkheid zit hoe dan ook in het dna van Triodos. Wij willen de maatschappij een beetje mooier, leuker, rechtvaardiger, sociale en groener te maken. Dan is er niks erger dan dat geld naar de verkeerde rolt, of misbruikt wordt." Dat geldt volgens De Jongh in dezelfde mate voor ABN AMRO. "Klanten verwachten van ons dat we zaken op een goede en fatsoenlijke manier aanpakken en dat we ons niet laten misbruiken voor verkeerde activiteiten."

MODUS OPERANDI Een van de grootste uitdagingen in het herkennen van crimineel geld is de veelheid van vormen waarin witwassen zich manifesteert. Het drietal noemt voorbeeld na voorbeeld. Denk aan het bekende Trade-Based Money Laundering waarbij handel en goederenstroom plaatsvinden die niet in verhouding staan tot de geldstromen die er onderliggen. Of aan georganiseerde netwerken met vele bankrekeningen die contant geld opnemen van de bankrekeningen waarop migrantenarbeiders uitbetaald worden.

>>

Dat soort patronen in beeld krijgen is uitermate complex, weet Rijpkema. Temeer daar alleen al bij de vijf bij TMNL betrokken banken tien miljard transacties per jaar uitgevoerd worden. “Uit al die transacties moeten de teams van Robin en Jane precies die transacties zien te vissen die ongebruikelijk zijn.” Die complexiteit maakt het extra belangrijk om samen op te trekken. “Samen zie je meer”, stelt De Jongh. “Zo weten criminelen precies dat systemen afgaan bij bepaalde bedragen. Dat omzeilen ze door de stortingen over meerdere banken te verdelen. Als individuele bank zie je dat niet.” Dat zelfde geldt voor geldstromen die over de grenzen heen door banken stromen. De Jongh: “Als geldstromen door diverse banken in diverse landen stromen en daar criminele netwerken onderliggen, zie je dat pas als je de modus operandi kent en het hele plaatje kunt bekijken.” Lobbrecht geeft aan dat er heel veel informatie nodig is om te kunnen zien dat geldstromen ongebruikelijk zijn. “Als je allemaal alleen maar kijkt naar een klein stukje van de keten, dan kan het zomaar zijn dat we dingen missen.”

TRANSACTIE MONITORING NEDERLAND De samenwerking binnen TMNL zien zij als een grote stap voorwaarts. Lobbrecht: “Daarachter zit de behoefte om meer data uit te wisselen en kennis en expertise te delen. Door samen te werken kunnen we bovendien efficiënter en effectiever gebruik maken van innovaties en nieuwe technieken als machine learning om patronen sneller te gaan herkennen.” Rijpkema verwacht dat de samenwerking gaat leiden tot een belangrijke verbetering in de effectiviteit van bestrijding van witwassen en terrorismefinanciering. “Doordat we zelf beter zicht krijgen op ongebruikelijke transacties zullen we als banken uiteindelijk kwalitatief betere informatie aanleveren bij de FIU.”
De verwachting is dat de groeiende expertise vanuit de samenwerking zal leiden tot minder zogenoemde ‘false positives’: transacties die de banken als ongebruikelijk zien, maar waarbij ze uiteindelijk zelf vaststellen dat ze dat toch niet blijken te zijn. Dat percentage wisselt per geldstroom, maar ligt nu gemiddeld rond de 95%. “Dat is vrij hoog”, beaamt Lobbrecht. “Maar elke extra stap die we zetten is waardevol. Door de samenwerking aan het begin van de keten denken we effectiever te worden.” Ze wijst erop dat een betere monitoring van transacties hoe dan ook een afschrikwekkend effect hebben. Rijpkema knikt. “Zeker. Op het moment dat je het als banken heel goed met elkaar organiseert, word je voor criminelen minder aantrekkelijk om te misbruiken. Men zoekt de zwakke plekken in het systeem. Als je als systeem je verdediging versterkt, heeft dat een preventieve werking.”

De vijf banken hebben het afgelopen jaar onderzocht hoe de samenwerking gestalte kan krijgen. Rijpkema verwacht dat deze zomer het besluit wordt genomen en TMNL dit najaar daadwerkelijk wordt opgericht.
TMNL komt als het ware boven de vijf deelnemende banken te hangen. De banken blijven aanvankelijk wel de eigen transactiemonitoring doen, maar op langere termijn wordt er gestreefd naar echte gezamenlijkheid. De Jongh: “In alle gevallen zullen de individuele banken overigens wel individueel verantwoordelijk blijven voor de transactiemonitoring. TMNL bepaalt alleen de vorm.”

PUBLIEK-PRIVATE SAMENWERKING
Samenwerking tussen banken is slechts de eerste stap in een meer integrale aanpak van crimineel geld, vertelt De Jongh.“Uiteindelijk moeten we dit doorontwikkelen zodat ook de overheid meedoet en we binnen de grenzen van privacy en informatie security nog effectiever data op elkaar kunnen leggen.” Ook op het gebied van publiek-private samenwerking (PPS) zijn mooie initiatieven gaande. Het drietal wijst op de diverse Task Forces en het Financieel Expertise Centrum (FEC) die zich hiermee bezig houden. De Jongh: “Ik was onlangs in Denemarken en daar zijn ze jaloers op hoe wij binnen de Serious Crime Taskforce binnen de mogelijkheden van de wet zorgvuldig informatie delen tussen publieke en private partijen. Natuurlijk kan het allemaal nog groter en kunnen we het verder professionaliseren, maar we mogen ons ook in de handen knijpen over wat wij al doen.” Lobbrecht geeft aan dat ook de mate waarin de overheid met wetgeving nu de samenwerking tussen de banken onderling probeert te faciliteren voor haar een positieve vorm van PPS is. “Ook dat kan allemaal sneller en beter, maar ik voel wel dat we, ook via de NVB, in voldoende mate worden uitgenodigd om in gesprek te zijn.”
Rijpkema wijst op het Nationaal plan aanpak witwassen dat de ministers van Financiën en van Justitie en Veiligheid vorig jaar lanceerden. “Hierin staat nadrukkelijk beschreven dat ze zich inspannen om gezamenlijke transac-

>>

tiemonitoring door de banken wettelijk mogelijk te maken. Er wordt hard gewerkt aan de noodzakelijke wetswijzigingen daarover.” Rijpkema verwacht dat daar dit najaar nadere stappen in gezet worden. “We slagen er met elkaar goed in om het gemeenschappelijk belang te waarborgen. Dat is een proces waarin je groeit en waar je geleidelijk aan ook meer wettelijke grondslag voor moet vinden. Ik denk dat dat zich goed ontwikkelt.”
De gesprekspartners zijn het er over eens dat naarmate er meer mogelijkheden komen om data te delen over de grenzen van banken, publieke partijen en zelfs landgrenzen heen, criminele netwerken steeds beter bloot gelegd kunnen worden.

Samen op zoek naar de speld in de hooiberg dus? Die beeldspraak leidt tot protest. Veel te negatief. Rijpkema: “Ik denk dat er veel reden is tot optimisme. Het gebruik van innovaties en moderne technologie maken dit onderwerp steeds beter beheersbaar.” De Jongh: “Tot twee jaar terug zei ik dat zelf ook nog wel zo, maar twee keer nu veel positiever. We trekken echt muren op. We maken echt het verschil.”
“Als we onze data, kennis en kunde combineren kunnen we het met zijn vijven nog ontegenzeggelijk beter doen”, vult Rijpkema aan. ”En we willen dit zo bouwen dat op termijn ook andere banken zich bij TMNL kunnen aansluiten. Met elkaar gaan we ons teweer stellen tegen het menselijk leed en de maatschappelijke ontwrichting die witwassen en terrorismefinanciering met zich meebrengen.” —

Transactie Monitoring Nederland In de strijd tegen witwassen en terrorismefinanciering onderzoeken ABN AMRO, ING, Rabobank, Triodos Bank en de Volksbank onder coördinatie van de Nederlandse Vereniging van Banken, de oprichting van *Transactie Monitoring Nederland* (TMNL). TMNL beoogt door het monitoren van een gecombineerde transactiedatabase van de verschillende banken mogelijke criminele geldstromen en netwerken beter te kunnen detecteren, dan wanneer banken dit individueel doen. Andere banken kunnen zich op termijn ook aansluiten. Naar verwachting nemen de betrokken banken deze zomer een besluit over de oprichting van TMNL.


Robin de Jongh


Jane Lobbrecht


Jeroen Rijpkema

BW
BANK|WERELD

INTERVIEW

Alleen Europese witwasaanpak kan tij keren

De huidige aanpak van financiële criminaliteit biedt criminele netwerken teveel kansen. Alleen een Europese witwasaanpak kan het tij nog keren. Een interview met Wim Mijs, *Chief Executive Officer* van de *European Banking Federation* (EBF), over de noodzaak fragmentatie in de regelgeving tegen te gaan en data-uitwisseling te bevorderen.

De EBF presenteerde 10 maart in het rapport Lifting the spell of dirty money een plan waarin gepleit wordt voor een Europese aanpak. Waarom is dit belangrijk? "Het is de enige manier om de strijd aan te gaan met criminele netwerken. We hebben te maken met boeven die de samenleving ondermijnen. Het gaat om mensen met geen enkel moreel besef, voor wie een mensenleven niet telt. Na de afgrijselijke moord op advocaat Wiersma zag je dat iedereen wakker werd. We kunnen dit niet laten lopen. Een Europese aanpak is daarbij essentieel."

Waarin schiet de huidige aanpak tekort? "In twee woorden: fragmentatie en data-uitwisseling. Je ziet – denk aan de schandalen in Letland en Denemarken vorig jaar – dat criminelen heel erg precies gebruik weten te maken van de fragmentatie van de regels in Europa."

Ze vinden de mazen in de wet? "Ik zou eerder zeggen: ze maken gebruik van de onhandigheden, dus van het feit dat de ene hand niet weet wat de andere doet. Die kans bieden we ze en daar moeten we mee ophouden."

De EBF wil blijkens het rapport af van de zes anti-witwasrichtlijnen uit Brussel en pleit voor verordeningen. Waarom werken de huidige richtlijnen niet? "De ruimte om die richtlijnen per lidstaat te interpreteren en vast te leggen in nationale wetgeving, zorgt ervoor dat bankfilialen in de verschillende landen anders omgaan met de meldingsplicht en de manier waarop ze naar witwaspatronen zoeken. *Laundromats* maken gebruik van die fragmentatie door BV's in verschillende landen op te richten en een systeem van schijnorders en schijnbetalingen op te zetten. Met een Europese verordening die direct toepasbaar is in alle lidstaten, zijn we beter in staat dit soort criminele netwerken te verstoren."

Waar zouden de door de EBF gewenste Europese supervisie in het toezicht en een EU-brede Financial Intelligence Unit ondergebracht moeten worden? "Het is in het toezicht op witwassen nodig dat er een autoriteit komt die met alle puzzelstukjes vanuit de verschillende lidstaten de hele puzzel kan leggen. Hoe je dat inricht maakt me niet zoveel uit. Belangrijk is dat je toezichthouders en opsporingsautoriteiten bij elkaar zet en ze het juiste mandaat en de *governance* geeft. Ik zou het liefst een nieuwe agency zien, maar ben me ervan bewust dat dat geld kost én dat er lidstaten zijn die allergisch zijn voor iedere extra bevoegdheid die naar Europa gaat. Maar er zijn meer opties."

Zoals? "Je kunt dit onderbrengen bij de *European Banking Authority* (EBA) of je versterkt het mandaat van Europol. Belangrijk is vooral dat er een gedeelde sense of urgency is om dit soort ontwrichtende netwerken aan te pakken. Zorg dat de regelgeving op orde komt, zorg dat je de AML-regels overal hetzelfde interpreteert, zorg voor voldoende opsporingsautoriteit, koppel terug, werk publiek en privaat goed samen en zorg dat er een plek is in Europa waar data gedeeld kunnen worden."

Wat verwacht de EBF in deze aanpak van de banken? "Je ziet dat *compliance*-afdelingen van banken steeds meer voor veilig gaan en voor de zekerheid enorm veel melden. Daarmee produceer je hooibergen waarin niemand meer de naald kan vinden. We moeten de banken helpen door meer feedback te geven om zo steeds preciezer te krijgen wie de echte criminelen zijn. Daarvoor hebben we een partij nodig die alle data naast elkaar legt. De Nederlandse aanpak met Transactie Monitoring Nederland (TMNL) is volgens mij precies goed. Financiën, Justitie, De Nederlandsche Bank en de afzonderlijke banken trekken hierin samen op. Dat is zo belangrijk."


Wim Mijs, Chief Executive Officer EBF

Een van de thema's in het rapport is het komen tot een internationale publiek-private aanpak. Ziet u de Nederlandse samenwerking in transactiemonitoring als een voorbeeld daarvan? "Zeker. In Europa wordt hier met veel belangstelling naar gekeken. We raken ervan doordrongen dat dit een strijd is die je niet in je eentje kan winnen. De publieke sector kan dat niet en de private niet. Als er één onderwerp is waar publiek-private samenwerking essentieel is, dan is het dit wel. Het is daarbij belangrijk dat je elkaar vertrouwt en hetzelfde doel voor ogen hebt. Dat maakt de aanpak binnen TMNL zo sterk. Als het lukt om dit juridisch met alle privacyregels helemaal kloppend te krijgen, dan zijn we op de goede weg."

Hoe ziet u de invloed van de huidige coronacrisis op de strijd tegen crimineel geld? "Het is een wetmatigheid dat criminelen hun weg vinden zodra een maatschappij is ontwricht door economische of sociale schokken. Het risico is dat een thema als de aanpak van crimineel geld in een crisis van deze omvang onder de oppervlakte verdwijnt. Ik hoop dat dat niet gebeurt. Het is van wezenlijk belang om de nietsontziende criminele netwerken te blijven verstoren."

Eind 2019 gaf NVB-voorzitter Chris Buijink aan dat de bestrijding van financiële criminaliteit een krachtig Europees antwoord vereist. Daar bent u het waarschijnlijk mee eens? "Absoluut, voor de volle honderd procent. Mede daarom is dit rapport er. De aanbevelingen in dit rapport vormen dat krachtige Europese antwoord. Als het in Nederland perfect op orde is dan ben je er nog niet, dan werken criminelen er gewoon omheen."

Heeft u er vertrouwen in dat het tij nog valt te keren? "Natuurlijk! Ten eerste ben ik van nature een optimist. Maar daarnaast voel ik in Nederland en binnen Europa de politieke wil om nu stappen te maken. Veel van onze aanbevelingen komen overeen met zaken waar ook de Europese Commissie mee bezig is. Een Europese aanpak vraagt bovendien niet direct om grote investeringen of ingrepen in de infrastructuur. Bijna alles is er al. De banken hebben al enorme *compliance*-afdelingen; de financial intelligence units zijn er al; Europol is er al; er zijn al tien mensen vrijgemaakt bij de EBA."

Er is dus weinig meer dat een Europese aanpak van witwaspraktijken in de weg staat? "Nee. Het komt vooral neer op het in orde maken van de regelgeving en een betere manier van samenwerken. Het uitvoeren van de aanbevelingen uit ons rapport vraagt om politiek leiderschap en lef." —

VOORJAAR 2020
Veiligheid

BW
BANK|WERELD

Veilig financieel ouder worden begint lokaal

De coronacrisis legt pijnlijk bloot hoe kwetsbaar ouderen zijn, ook als het gaat om financiële uitbuiting. Banken werken samen met andere private en publieke partijen in een groeiend aantal lokale allianties. "Met veel disciplines dicht op de doelgroep: dat werkt goed."

Naar schatting zijn per jaar dertigduizend ouderen slachtoffer van financieel misbruik. Vaak begint het onschuldig, zegt Marianne van der Krans, projectsecretaris van de landelijke netwerkorganisatie Veilig Thuis. "Een dochter stelt voor een en/of-rekening te openen met het argument dat ze het geld voor de boodschappen dan niet hoeft voor te schieten. Of als het slechter met moeder gaat ze de financiën makkelijker kan overnemen. Als ze zelf wat krap zit, is het verleidelijk af en toe wat geld van moeders rekening over te schrijven." De zelf opgenomen bedragen worden sluipenderwijs hoger totdat de rekening zo is geplunderd dat moeder de huur niet meer kan betalen en de woningbouwvereniging aan de bel trekt.
Veilig Thuis zet zich in tegen huiselijk geweld en mishandeling, waaronder ook financiële uitbuiting van ouderen valt. Ons land telt 26 regionale Veilig-Thuisorganisaties ook die met elkaar voortdurend werken aan verbetering van de kwaliteit van hun werk. Daartoe hebben zij zich verenigd in het Landelijk Netwerk Veilig Thuis. Zowel slachtoffers, plegers als professionals kunnen contact opnemen met Veilig Thuis.
Slachtoffers van financiële uitbuiting zijn meestal vrouw, ouder dan 80 jaar, alleenwonend en hebben vaak een klein netwerk. De plegers zijn meestal mantelzorgers, vaak familieleden. De afhankelijke relatie maakt bestrijding van financieel misbruik lastig, zegt Van der Krans. "Slachtoffers schamen zich dat ze niks in de gaten hadden. Of ze praten het goed: mijn zoon kan wel een extraatje gebruiken nu hij zoveel voor mij doet, mijn dochter heeft het al zo moeilijk." En bovendien: wat gebeurt er als er echt een zaak van wordt gemaakt? Valt de zo welkome ondersteuning voor de oudere dan weg? Het gevolg is dat slachtoffers er vaak niet mee naar buiten willen treden en liever een oogje toeknijpen. Totdat de gevolgen soms niet meer te overzien zijn. Soms is een eerste gesprek een wake up-call, is de ervaring van Van der Krans. Dan ontkent iemand aanvankelijk dat er iets aan de hand is, maar melden zich een half jaar later alsnog omdat de schulden zijn opgelopen of beseffen ze dat er inderdaad misbruik van ze wordt gemaakt.
Sinds vorig jaar heeft Veilig Thuis een directe lijn met een medewerker van alle grootbanken. Alle organisaties van Veilig Thuis kunnen contact opnemen via dit meldpunt om een geval van mogelijke financiële uitbuiting te bespreken of advies te vragen. Dat gaat op anonieme basis, verzekert Jasper Grotjohann, senior Business Expert van ABN AMRO. "Zo kwam er vanuit Veilig Thuis onlangs een vraag of het mogelijk is op een betaalpas pinacties te blokkeren omdat men financieel misbruik vermoedde. De naam van de rekeninghouder wordt dan niet genoemd." Een ander voorbeeld: een organisatie van Veilig Thuis geeft, na toestemming, naam en adres van een bankrekeninghouder door aan de bank met de vraag of de bank het 'niet-pluis-gevoel' deelt. Grotjohann: "Het enige dat we na onderzoek antwoorden is 'ja' of 'nee'. We geven geen bijzonderheden door over het financieel gedrag van de klant."
Ook voor bankmedewerkers is het signaleren van financieel misbruik niet eenvoudig, zegt Roxana Faujdar, productmanager wonen van Rabobank. "Als een oudere klant aan de balie komt met haar zoon voor een volmacht en je vertrouwt het niet. Wat doe je dan? Welke vragen moet je stellen? En wat als je vraagtekens plaatst bij transacties op een rekening?" Onder de vlag van de Nederlandse Vereniging van Banken (NVB) is daarom een e-learning ontwikkeld voor alle bankmedewerkers hoe ze signalen kunnen herkennen en welke stappen ze kunnen ondernemen.
Nederlandse banken hebben de afgelopen jaren verschillende stappen gezet om financiële uitbuiting van ouderen terug te dringen. In 2018 sloten de NVB en het ministerie van Volksgezondheid, Welzijn en Sport (VWS), een convenant over veilig financieel ouder worden. De banken spraken af te zorgen voor duurzame borging van kennis binnen hun organisatie en medewerkers te trainen in het herkennen van signalen. De e-learning is daarvan onder andere het resultaat. In voorlichting aan klanten wordt gewezen op maatregelen die financieel misbruik helpen te voorkomen. Zoals het openen van een huishoudrekening, het verlagen van de paslimiet en bij overschrijvingen een gemachtigde laten meekijken: het 'vier-ogen-principe'. Een doorslaand succes is de Informatiebox Financieel Veilig Ouder Worden, gemaakt in samenwerking met het ministerie van VWS. Door de grote vraag tijdelijk alleen online te raadplegen. Landelijk werken de banken samen met externe partners in de Brede Alliantie Veilig Financieel Ouder worden, in 2015 opgericht op initiatief van het ministerie van VWS. Op lokaal niveau zijn de banken een belangrijke partner in het groeiende aantal lokale allianties. Private en publieke partijen zoals politie, notarissen, wijkverpleegkundigen, Veilig Thuis, ouderenbonden, gemeente en de banken trekken daarin gezamenlijk op

>>

en weten elkaar door de korte lijntjes snel te vinden. “Verschillende disciplines en dicht op de doelgroep: dat werkt goed”, weet Roxana Faujdar. “Op basis van casussen wisselen we ervaringen uit, signaleren we financiële uitbuiting en ondernemen we actie.” Zelf is ze aangesloten bij de lokale alliantie in haar woonplaats Zoetermeer. Daar ziet ze de resultaten. “We hebben financieel misbruik onder patiënten van een huisartsenpraktijk gemonitord. In drie kwartalen zijn daar 35 casussen opgelost.” Grotjohann beaamt de kracht van lokale samenwerking vanuit zijn ervaringen in zijn woonplaats Alphen aan de Rijn. “Daar heeft de politie onze e-learning voor financieel misbruik gedeeld met wijkagenten, die daardoor veel alerter zijn op het thema. Kennisvergroting van professionals zoals hier draagt bij aan het oplossen van het probleem.” Banken leren overigens ook van professionals in het veld, voegt hij daaraan toe. “Dat er gevoelens van schaamte spelen bijvoorbeeld, of hoe mistig een gezinsstructuur kan zijn. Het delen van die ervaring en kennis helpt ons beleid te maken.” De coronacrisis legt pijnlijk bloot hoe kwetsbaar ouderen zijn, ook als het gaat om financieel misbruik. Van der Krans: “Het gaat vooral mis bij mensen met weinig contacten. Als je drie hoog op een flatje zit ben je al lang blij dat de buurvrouw aanbiedt iets voor je mee te nemen van de supermarkt. Je geeft dan net wat makkelijker je pasje mee, ook omdat veel winkels geen contant geld meer accepteren.” Grotjohann oppert te onderzoeken of er alternatieven zijn voor een betaalpas. “Een wijze van betalen op een wettige manier die voor iedereen veilig is. Daar zouden we mee aan de slag moeten”. Hij glimlacht. “Het is een groot pluspunt dat zoveel partijen nu samenwerken, maar er is nog veel te winnen.” —

Marianne van der Krans, Jasper Grotjohann en Roxana Faujdar

WAT DOEN DE BANKEN?

RABOBANK

» Seniorenadviseurs bezoeken ouderen, visueel beperkte en laaggeletterde klanten.
» Platform ikwoonleefzorg met artikelen over financieel misbruik: https://www.ikwoonleefzorg.nl/financien/wat-kunt-u-doen-aan-financieel-misbruik
» Deelname aan 76 lokale allianties om ook lokaal financieel misbruik bij ouderen te voorkomen. Voor meer informatie zie: https://www.youtube.com/watch?v=nD-MY6x_99WU&t=18s

ABN AMRO

» Financiële zorgcoaches gaan langs bij klanten die niet mobiel zijn om te ondersteunen bij dagelijkse bankzaken. Een laagdrempelige manier om ook te adviseren over voorkomen van financieel misbruik.
» Met steeds minder klantcontacten op kantoor wint de seniorenlijn aan belang. Klanten bellen de bank en de bank belt de klanten. “Een mooie bijkomstigheid van het bellen is dat de ouderen even een praatje kunnen maken, waardoor zij zich op dat moment minder eenzaam voelen,” vertelt Nery Anderson, directeur Dagelijkse Bankzaken bij ABN AMRO. “Dat wordt door de klanten zeer gewaardeerd”.

DE VOLKSBANK

» Proactief contact opnemen met de oudere klanten en deze klanten bellen om te toetsen of er hulp nodig is bij de dagelijkse bankzaken.
» Workshop Webwijs.
» Workshop Veilig Online Bankieren.

BW
BANK|WERELD

GASTCOLUMN

SAMEN WERKEN AAN CYBERVEILIGHEID

WIM HAFKAMP OVER HET VERHOGEN VAN DE CYBERWEERBAARHEID

De opkomst van de informatietechnologie (ICT) betekende ook de opkomst van ‘de cybercrimineel’. Bij veel ondernemingen in de financiële sector gingen ICT en informatiebeveiliging vanaf het begin hand in hand. Hoe kun je informatie het best beschermen? Welke risico’s en trends zijn er en hoe speel je daarop in? De komst van internetbankieren bracht weer nieuwe risico’s en technieken met zich mee, zoals phishing, malware en computervirussen. Banken werkten al snel onderling samen om kennis over cyberveiligheid te delen. Banken zijn een goed georganiseerde sector als het gaat om cyberveiligheid en data-uitwisseling om *cybercrime* tegen te gaan. De strijd tegen *cybercrime* is voor elke bank dezelfde. Dat is denk ik echt een voorbeeld voor andere sectoren.”

“Publiek-private samenwerkingen waarbij gegevens met overheidsorganisaties worden gedeeld om *cybercrime* tegen te gaan, zijn wat jonger maar zeker succesvol. Bij het vrij jonge Z-CERT ben ik verantwoordelijk voor het verhogen van de cyberweerbaarheid in de Nederlandse zorgsector. Een sector die formeel niet als ‘vitaal’ is verklaard en daarom nu geen beroep kan doen op het *Nationaal Cyber Security Centrum*. Maar natuurlijk moet je er niet aan denken dat een IC-afdeling van een ziekenhuis plat komt te liggen omdat het systeem wordt gehackt. Dus de sector is wel van cruciaal belang voor de samenleving. Z-CERT helpt op dit moment ziekenhuizen en GGZ-instellingen bij het voorkomen en oplossen van cyberincidenten. Ons werk gebeurt vooral ‘onder de motorkap’: welke actuele dreigingen en kwetsbaarheden zijn er in de informatiesystemen van deelnemers? Zien wij iets, dan sluizen we dat zo snel mogelijk door naar de betreffende instellingen. Daarbij geven we ook aan hoe ze die kwetsbaarheden kunnen verhelpen. Soms moeten hele systemen uitgezet worden, omdat de risico’s op bijvoorbeeld een DDoS-aanval of gegevenslek te groot worden.”

“Wat de zorg en de financiële sector van elkaar zouden kunnen leren? Ik ben blij verrast over de enorme samenwerkingsbereidheid binnen de zorg. Binnen de financiële sector is er weliswaar een Financial-CERT, maar die kent nog weinig deelnemers en het samenwerkingsverband staat ook (nog) niet op eigen benen. Aan de andere kant zijn de middelen in de zorgsector schaarser. Dat zie je terug in de capaciteit voor maatregelen tegen complexe cyberdreigingen. Banken zijn vanaf het begin van de digitalisering doelwit geweest van cybercrime, daar leer je van en daar pas je je maatregelen op aan. Ik stond zelf aan de basis van het programma *Threat Intelligence Based Ethical Red Teaming* (TIBER). Daarbij worden onder leiding van De Nederlandsche Bank aanvallen op financiële systemen nagebootst om te kijken of die gedetecteerd worden. Dat is iets waarvan ik zeg: ik wou dat we als zorgsector zo ver waren. Misschien dat de banken de zorg daar ook in zouden kunnen helpen? Dan zou de zorg op haar beurt ervaringen kunnen delen met het inrichten van een sectorale CERT voor de hele financiële sector in het kader van de goede samenwerking.” —

Dr. Wim Hafkamp, managing director Z-CERT (Computer Emergency Respons Team)

Plofkraken is een hardnekkig en ontwrichtend fenomeen.

Strijd tegen plofkraakcrimineel vergt maatwerk

Samenwerking tussen banken en publieke partijen leidt tot veelbelovende maatregelen, vertellen Job Galesloot (ING) en Peggy Corstens (Geldmaat).

BW
BANK|WERELD

Weinig mensen hebben waarschijnlijk zoveel plofkraken meegemaakt als Job Galesloot, security officer bij ING. In een proefomgeving, welteverstaan. Een plofkraak is geen explosie, legt hij uit, maar een aanval met een gasmengsel van acetyleen en zuurstof. “Dat veroorzaakt een extreme ontbranding, klinkend als een enorme plof. Vandaar de naam.” De wijze waarop kluizen worden gekraakt is in de loop der tijd veranderd. Aan plofkraken gingen ramkraken en trekkraken vooraf. Galesloot: “Vroeger trokken ze de automaat met een trekker uit de muur.” Hij lacht. “Dan kreeg ik een belletje van een boer: ik heb in mijn weiland zo’n ding liggen, open gezaagd en wel. Wat moet ik ermee?” Inmiddels zijn in Nederland ook gaskraken passé. De moderne crimineel gebruikt een explosief. Met enorme materiële schade én veiligheidsrisico’s voor omwonenden tot gevolg.

Galesloot is als voorzitter van de Expertpool Fysieke Incidenten, onder de vlag van de Nederlandse Vereniging van Banken (NVB), nauw betrokken bij de strijd tegen plofkraakcriminelen. Het aantal plofkraken fluctueert per jaar (vorig jaar waren het er 71), maar blijft een hardnekkig fenomeen. “Dat komt omdat er een verwachting is dat de kraak iets oplevert”, zegt Galesloot. Hij trekt een vergelijking met het kopen van een staatslot. “Je hebt misschien nog nooit iets gewonnen, maar je blijft er een kopen. Omdat er een kans is dat je iets wint. En je accepteert het als het niet zo is. De dader van een plofkraak denkt: ik kan ernaast grijpen, maar ik kan ook met een zak geld vertrekken. Zolang die verwachting er is, kun je aanvallen verwachten.”

Peggy Corstens, chief service officer bij Geldmaat, wijst op verharding in het criminele circuit. “Jonge mensen die voor relatief weinig geld best heftige acties ondernemen en niet terugdeinzen voor de risico’s.” Galesloot beaamt dat. “Een deel van de daders gaat systematisch te werk, hun gedrag is extreem instrumenteel, ze weten precies wat ze doen. En de buit wordt onder andere geïnvesteerd in andere criminele activiteiten.” Krachtigere middelen van de criminelen worden steevast gevolgd door nog sterkere kluizen en andere beveiligingen door de banken. Waarop de plofkrakers weer een antwoord vinden. Een eindeloze wedloop. Corstens: “Nog zwaardere kluizen installeren heeft geen zin meer.”
Geldmaat begon in juni vorig jaar met het plaatsen van de nieuwe gezamenlijke geldautomaten van ING, ABN AMRO en Rabobank. Doel van de maatregel is de geldautomaten evenwichtiger te spreiden. Bestaande automaten worden omgebouwd, verplaatst of verwijderd, nieuwe automaten worden bijgeplaatst. Vooral in drukke dorps- en stadscentra, waar vaak meerdere geldautomaten op korte afstand van elkaar staan, worden geldautomaten ‘ontdubbeld’. Door de coronacrisis stokt de teller nu even op ruim duizend geplaatste automaten maar de verwachting is dat begin 2021 alle gele automaten geplaatst zijn. Het aantal indoor geldautomaten groeit, omdat mensen het volgens Corstens prettiger vinden om binnen te pinnen en vanwege de veiligheid. “Je kunt daar inderdaad ’s avonds niet terecht, maar mensen hebben daar begrip voor. En er blijven ook gevelautomaten in het straatbeeld. We kijken goed naar de bereikbaarheid, beschikbaarheid, in combinatie met veiligheid.”
In een landelijk overleg tussen de banken en de ministeries van Financiën en Veiligheid & Justitie zijn afspraken gemaakt die het aantal plofkraken moeten terugdringen. De banken onderzoeken samen met gemeenten en politie waar geldautomaten een risico vormen en of ze verplaatst kunnen worden.
In Nederland moeten consumenten binnen een straal van vijf kilometer toegang hebben tot een geldautomaat. Andere plaatsingscriteria zijn het aantal transacties, piekmomenten (bijvoorbeeld een winkelstraat op een drukke zaterdag) en de omgeving (bijvoorbeeld een uitgaanscentrum of winkelcentrum waar geld wordt uitgegeven). “Er is altijd een spanningsveld tussen veiligheid en het beschikbaar houden van contant geld”, ervaart Corstens in haar werk. “Natuurlijk zijn mensen chagrijnig als er een geldautomaat wordt verplaatst of verdwijnt. Lokale ondernemers hebben baat bij een geldautomaat in de buurt, ook voor het afstorten van geld.” Daarentegen zijn er ook burgers en lokale bestuurders die de geldautomaat liever zien gaan dan komen, omdat ze het onveilig vinden.

Corstens: “We stellen ook de vraag of een geldautomaat na een plofkraak

>>

moet terugkeren. Dat hoeft soms niet omdat er genoeg alternatieven in de omgeving zijn. Het is altijd maatwerk. De ene situatie is de andere niet. Een houten woning in een drukbevolkt gebied vergt andere afwegingen dan een solide gebouw in een winkelcentrum." Galesloot vult aan: "We overleggen met gemeenten."

Daarnaast zijn alle geldautomaten sinds 16 december vorig jaar gesloten tussen elf uur 's avonds en zeven uur 's ochtends. Uitzondering vormen zo'n honderd geldautomaten die 's nachts relatief vaak worden bezocht: uitgaand publiek kan daar nog tot twee uur 's nachts terecht. De maatregel lijkt effect te sorteren, antwoordt Corstens desgevraagd. "Er is een sterke reductie in het aantal plofkraken." Galesloot vermoedt dat vooral de 'copy cats' en de amateurs ontmoedigd zijn, de kleinere jongens. "De nachtsluiting heeft beperkte gevolgen voor de bereikbaarheid en beschikbaarheid van contant geld. Minder dan twee procent van alle geldopnamen bij automaten die buiten staan, gebeuren 's nachts. Uit onderzoek in opdracht van de NVB en de Betaalvereniging Nederland bleek dat vrijwel alle Nederlanders begrip hebben voor de nachtsluiting." Tot slot werken banken, Geldmaat, De Nederlandsche Bank en de politie aan een techniek om bankbiljetten bij een plofkraak onbruikbaar te maken. Het ontwaarden van geld lijkt een veelbelovend middel om een einde te maken aan de 'wapenwedloop' tussen plofkraakcriminelen enerzijds en publiek-private partijen anderzijds. Corstens verwacht dat de techniek vanaf eind dit jaar kan worden toegepast. De nachtsluiting van geldautomaten kan dan in principe worden opgeheven.

Opsporing en vervolging van daders gaan onverminderd door. De banken en Geldmaat voorzien de politie en het Openbaar Ministerie zo nodig van informatie voor speciale plofkraakteams die ook internationaal samenwerken. In Europa is Nederland overigens voorloper als het gaat om kennis over plofkraken, weet Galesloot, die voor ING en de sector samen met politie meepraat in een Europees platform. "Wij hebben een hoog kennisniveau over plofkraken, welke middelen er worden gebruikt en welke maatregelen welk effect sorteren." De publiek-private samenwerking van ministeries, politie en banken in Nederland is volgens hem in Europa uniek op dit gebied en ervaart hij als waardevol in de strijd tegen plofkrakers. "De politie helpt de banken in dit opzicht uitstekend en is een goede toetssteen en sparring partner."

Wat de gevolgen van de coronacrisis op het gebruik van de geldautomaten zal zijn, moet de toekomst uitwijzen. De opname van contant geld halveerde de afgelopen weken. Geldmaat verwacht dat 'een deel van het verkeer' terugkomt. Corstens: "Als bijvoorbeeld ouderen weer boodschappen doen, kan het zijn dat ze toch weer contant betalen. Maar een deel van de daling zal blijvend zijn. In elk geval zorgt Geldmaat ervoor dat contant geld goed bereikbaar blijft." Galesloot constateert dat 'digitale inclusie' door de coronacrisis meer aandacht krijgt. "Dat is goed nieuws voor ons en slecht nieuws voor plofkraakcriminelen." —

Links Peggy Corstens, chief service officer bij Geldmaat. Rechts Job Galesloot, security officer bij ING

BW
BANK|WERELD

Leonie Bik Specialist Wwft

Competence Center Klantintegriteit (CCKI) van De Volksbank

Kun je iets vertellen over wat het CCKI doet? "Bij het CCKI houden we ons bezig met allerlei aspecten van integriteit van bestaande klanten van onze vier labels. Op het thema transactiemonitoring werken we dagelijks met enkele tientallen collega's. We monitoren alle rekeningen, maar kunnen natuurlijk niet elke rekening en elke transactie separaat bekijken. Ons systeem bepaalt welke rekening van een klant 'op popt' en welke transactie(s) daarop ongebruikelijk is. Zo'n alert leidt tot een eerste onderzoek. Is die transactie werkelijk ongebruikelijk? Wat gebeurt er nog meer op die rekening? Past de transactie wel of niet bij het klantbeeld van die klant? Zien we ongebruikelijke zaken die we niet kunnen thuisbrengen, dan volgt een nader onderzoek en eventueel een melding aan *Finance Intelligence Unit* (FIU) NL."

Wat houdt jouw functie als specialist Wwft precies in? "Ik houd me niet zozeer bezig met het operationele transactieonderzoek, dus ik kijk niet zozeer of een transactie wel of niet ongebruikelijk is. In mijn functie ben ik verantwoordelijk voor het opstellen van goede 'scenario's' zoals wij dat noemen. Scenario's die ervoor moeten zorgen dat ons systeem – de juiste – meldingen 'bovenhaalt' op bepaalde integriteitsrisico's in het kader van de Wwft. Het gaat dan om aanwijzingen voor bijvoorbeeld mensenhandel, witwassen of terrorismefinanciering. Indicaties op een rekening kunnen bijvoorbeeld zijn grote contante stortingen of dito opnames. Of juist transacties met hoog-risicolanden."

Wat vind je het leukste aan je werk? "Onderzoek is een belangrijk deel van mijn werk, en ook het allerleukste deel vind ik. Want het is niet alleen belangrijk dat we scenario's hébben. Maar ook dat ze detecteren op de risico's die vóórkomen. Hebben we die allemaal in beeld, dus hebben we daar een scenario voor? Verder moeten de scenario's ook werken. Ze moeten inderdaad alle of zo veel mogelijk ongebruikelijke klanten 'naar boven halen'. Aan de andere kant moeten we ook opletten dat onze scenario's niet te veel valse meldingen opleveren. Ik zorg dus naast het testen van scenario's dat ze achteraf getoetst worden. Ook duik ik nog steeds graag in cases om te kijken of een scenario juiste alerteert."

Werken banken nauw samen in transactiemonitoring? "Ja, er zijn verschillende initiatieven, zoals de Fintel Alliance die nu wordt opgezet. Dit samenwerkingsverband komt voort uit een pilot van de Volksbank en FIU-NL. Doel is om kennis, informatie en ervaringen te delen. De vier grootbanken hebben samen een groot deel van het klantbestand van Nederland. Werk je samen, dan kun je dus als sector effectiever werken in de strijd tegen witwassen en andere delicten. Ook ben ik betrokken bij publiek-private samenwerkingsverbanden op specifieke onderwerpen, zoals mensenhandel."

Wanneer ben je blij met de resultaten van je werk? "Inhoud staat bij mij voorop. Dus als wij als Wwft-specialisten bepaalde fenomenen goed kunnen detecteren in onze systemen en het cases oplevert die voor onze collega's interessant en relevant zijn om te onderzoeken, dan ben ik een tevreden mens."

Criminelen zijn inventief en weten telkens weer in te spelen op een crisissituatie, zoals nu bij het coronavirus. ***Laurine van Teulingen,*** *fraude-expert bij ABN AMRO, zoekt naar wegen om ze een stap voor te blijven. Een gesprek over het navigeren binnen de privacywetgeving, de meerwaarde van samenwerken en de wens om te komen tot een integrale aanpak.*

FRAUDE IN HET BETALINGSVER-KEER

U bent adviseur binnen de afdeling Security & Integrity van ABN AMRO. Waarmee houdt u zich bezig? "Banken monitoren het transactieverkeer en als er een vermoeden ontstaat van fraude, wordt dat realtime onderzocht. Als er daadwerkelijk sprake is van fraude, worden er direct maatregelen getroffen. Daarna kijken we wat we in de eigen processen van de bank kunnen verbeteren, zodat we deze vorm van fraude een volgende keer kunnen voorkomen of sneller maatregelen kunnen treffen. Ik adviseer het management over hoe we onze processen slimmer en veiliger kunnen inrichten."

Fraudebestrijding klinkt als een spannend vak. Klopt dat? "Zeker, hoewel het zoeken naar de speld in de hooiberg ook heel taai kan zijn. Het werkveld is complex, er worden miljoenen transacties per week verwerkt en fraudeurs passen steeds hun werkwijze aan. Als fraude-expert moet je steeds opnieuw het wiel uitvinden en blijf je leren. Het geeft veel voldoening als je daadwerkelijk iets vindt en vervolgens de processen binnen de bank kunt verbeteren. Ik ben heel trots op mijn werk."

Hoe ziet de samenwerking tussen banken en met andere partijen eruit? "Onder strikte voorwaarden kunnen we fraude melden aan andere banken en laten opnemen in het externe verwijzingsregister. We werken in de opsporing samen binnen verschillende Taskforces. Zo is er de Electronic Crimes Taskforce en sinds vorig jaar de Serious Crime Taskforce waarbinnen de banken samenwerken met OM, politie, FIOD en FIU-NL. Binnen de wettelijke kaders wordt daarin informatie uitgewisseld en samen onderzoek gedaan. Dit is heel belangrijk, want een crimineel maakt het niets uit bij welke bank iemand bankiert."

Wat ziet u als belangrijkste uitdaging voor de fraudebestrijders van de banken? "Dat is zonder meer het opereren binnen de regels van de privacywetgeving. Banken in Nederland moeten meer doen om de privacy van klanten te beschermen dan ze mogen doen om fraude te bestrijden. Een vermoeden van fraude mag je op basis van privacywetgeving niet neerleggen bij andere banken en je mag dan geen persoonsgegevens over de vermeende fraudeur uitwisselen. Daardoor kun je niet altijd goed verifiëren of je vermoedens juist zijn. Dat is voor ons erg lastig, vooral omdat je juist snel wilt acteren. Als je geen verificatie kunt doen, blijft het soms bij een vermoeden."

Frustrerend? "Ja, dat is soms echt wel frustrerend. Er zit een spanningsveld tussen onze uitvoeringsplicht als bank en onze rol om fraude te voorkomen. We kunnen klanten wel waarschuwen dat ze mogelijk het slachtoffer worden van oplichting. Maar als een klant desondanks toch een betaling wil laten doorgaan, zijn we verplicht om die uit te voeren. Als achteraf blijkt dat je vermoeden klopt, is het te laat. Het geld is al weg."

Welke vormen van fraude op het gebied van het betalingsverkeer komt u tegen? "Er zijn diverse vormen van cybercrime. Bekend is phishing, waarbij een fraudeur via een valse e-mail of link of via een valse website vertrouwelijke informatie van een slachtoffer bemachtigt. De landelijke schade door phishing naar beveiligingscodes voor internetbankieren bij bankklanten is vorig jaar meer dan verdubbeld, van 3,81 miljoen euro in 2018 tot 7,94 miljoen euro in 2019. Ook zijn er criminelen die kwaadaardige software instaleren op iemands computer. Deze zogenoemde malware kan betalingen onderscheppen. En een vorm van fraude wat voor de bank heel moeilijk te zien is, is oplichting. Het gaat dan om betalingen die klanten van de bank zelf doen, waarbij ze achteraf misleid blijken te zijn."

Kunt u voorbeelden noemen van dit soort oplichting? "Denk aan Marktplaats-oplichting waarbij je betaalt voor iets wat je nooit ontvangt. Of aan dating-fraude, waarbij je denkt iemand goed te hebben leren kennen en vervolgens in gaat op een verzoek om geld. Ook bedrijven worden slachtoffer van oplichting: bijvoorbeeld bij de zogeheten CEO-fraude. Hierbij denkt een medewerker dat zijn CEO een verzoek doet om betaling. Uiteindelijk komt het er op neer dat een crimineel het vertrouwen van een slachtoffer weet te winnen."

Zien jullie door de coronacrisis een verschuiving in het soort fraude dat optreedt? "We zien nu vooral veel oplichting via social media. De fraudeur doet zich via WhatsApp voor als een familielid met zogenaamd een nieuw nummer en vraagt 'pap' of 'mam' om geld over te maken. Dit soort vormen van oplichting zijn van alle tijden, maar we zien nu door de coronacrisis echt een toename. Ook zien we nu fraudeurs die zich voordoen als partij die handgel of mondkapjes verkopen aan particulieren of bedrijven. Hierbij kan het om grote bedragen gaan."

Hoe verklaart u die toename? "Fraudeurs spelen graag in op de actualiteit. Het coronavirus zorgt voor een periode met veel onzekerheid, angst en zorgen en daar maakt een fraudeur misbruik van. Hij speelt in op gevoelens van bezorgdheid en hulpvaardigheid. Die ouder die toch al ongerust is over zijn kind. Of de persoon die graag goed wil doen en ingaat op een beroep om zijn hulp. Fraudeurs winnen je vertrouwen en zorgen er door er spoed achter te zetten voor dat je impulsief reageert."

Hoe kun je als bank je klanten wapenen tegen fraudeurs? "We detecteren frauduleuze transacties en nemen hier maatregelen op. We houden trends bij en wijzen onze klanten daar zoveel mogelijk op. We zorgen ervoor dat de informatie over fraudetrends op onze website steeds actueel wordt gehouden. We beschrijven voorbeelden en geven tips over waarop je moet letten om te voorkomen dat je slachtoffer wordt van oplichting of fraude. We wisselen ook informatie uit over trends en de werkwijze van fraudeurs met andere banken en opsporingsinstanties, zodat we met elkaar kunnen werken aan meer bewustzijn."

Tot slot, wat staat er op uw wensenlijstje als het gaat om het nog beter bestrijden van fraude? "Ik zou er heel graag naar toe willen dat fraude integraal wordt bestreden in combinatie met andere vormen van financiële economische delicten. Er zit veel overlap tussen fraude, corruptie en witwassen. Een crimineel komt op verschillende manieren aan zijn geld, en als hij dit eenmaal heeft moet hij het ook witwassen. Dit zijn geen aparte circuits. Onze aanpak zou veel krachtiger worden als we dit integraal gaan aanpakken." —

BW
BANK|WERELD

VOORJAAR 2020
Veiligheid

Corona *Monitor*

*Banken hebben ruim 149.000 ondernemers geholpen en 31.000 consumenten hebben financieel meer lucht gekregen**

De coronacrisis doet iedereen pijn. Hij raakt de gezondheid van velen en trekt een zware wissel op de economie.

Duizenden bankmedewerkers doen alles wat onder deze omstandigheden mogelijk is, door veel klanten uitstel te geven van betalingen en extra krediet te bieden, in aanvullingen op de maatregelen van de overheid.

De banken doen wat nodig is om samen gezond uit de crisis te komen.

Elke twee weken brengen we de **Corona Monitor** uit die inzicht geeft in de bancaire financieringen aan ondernemers en consumenten.

Kijk op www.nvb.nl/coronamonitor

**Corona Monitor* 12 juni 2020*

Nederlandse Vereniging van Banken

Lees ook
Bank|Wereld Online