REACTIE ABN AMRO:

- Hoeveel klanten van ABN Amro zijn de afgelopen maanden slachtoffer geworden van spoofing fraude? Dat is niet met zekerheid te zeggen. Helaas melden niet alle slachtoffers zich bij de bank of bij de politie. Wel hebben we de afgelopen tijd, mede vanwege corona, een toename gezien van het aantal meldingen. In totaal gaat het om tussen de 10-20 gevallen per week.
- Heeft ABN Amro de schade van de spoofing fraude in sommige gevallen vergoed aan klanten, waarom wel/niet? Bij spoofing trapt de klant in de oplichtingstruc van de crimineel. De dader weet het slachtoffer op geraffineerd wijze ervan te overtuigen om geld over te maken. De bank vergoed geen schade als gevolg van spoofing, omdat de het slachtoffer zelf de overboeking heeft gedaan. Wel is het belangrijk om zo snel mogelijk melding te doen bij de bank van oplichting. Alleen dan kunnen banken onderling actie ondernemen om eventuele tegoeden op de rekening van de begunstigde (meestal een 'geldezel') te bevriezen en mogelijk nog verdere schade te voorkomen. In sommige gevallen is het overgemaakte geld nog niet cash opgenomen of weggesluisd naar elders en kan (een deel van) het geld in dat geval alsnog worden teruggegeven aan het slachtoffer.

- Weet ABN Amro op dit moment precies wat er gebeurt tijdens deze oplichting? Wordt er bijvoorbeeld door de oplichter ook live meegekeken in de rekening van de het slachtoffer op het moment dat de spoofing fraude plaatsvindt? Door meldingen van klanten en samenwerking met autoriteiten hebben banken inzicht in de manier waarop spoofing vaak plaatsvindt. De dader kijkt bij spoofing niet mee op de rekening van de klant, maar overtuigt de klant ervan geld over te maken naar een rekening van een derde. Er zijn wel andere vormen van internetcriminaliteit zoals phishing, waarbij het doel van de criminelen is om inlogcodes te bemachtigen. Daarmee kan de crimineel controle krijgen over de rekening van de klant. Een combinatie van de twee kan ook voorkomen. Daar kennen we helaas ook voorbeelden van. Dan wordt een klant bijvoorbeeld gebeld door "de bank" en ontvangt tijdens het gesprek smsje van "de bank" met "u bent nu in gesprek met een medewerker van de bank, klik hier voor bla bla". Dat linkje gaat naar een phishingsite, waarmee de fraudeur zich toegang verschaft tot de rekening van het slachtoffer terwijl hij/zij nog aan de lijn hangt met klant. De fraudeur ziet het saldo en overtuigt de klant met die kennis om gelden zelf verder over te boeken.

- Hoe en wanneer heeft ABN Amro klanten gewaarschuwd voor deze spoofing fraude? Maakt het in de overweging om schade wel of niet te vergoeden uit of iemand ten tijde van de spoofing fraude wel of geen waarschuwing vanuit de ABN Amro heeft ontvangen over het bestaan van deze spoofing fraude? ABN AMRO waarschuwt al geruime tijd voor diverse vormen van internetcriminaliteit. Dat doen we op onze website, bijvoorbeeld voor spoofing: https://www.abnamro.nl/nl/prive/abnamro/veilig-bankieren/fraude-herkennen/telefonische-oplichting.html. Maar ook voor andere vormen van internetcriminaliteit. Zie: https://www.abnamro.nl/nl/prive/abnamro/veilig-bankieren/index.html en de gezamenlijke website van de NVB en de Betaalvereniging Nederland en via campagnes op radio en tv. Voor een recente uitspraak over spoofing en een klacht over de voorlichting van de bank zie: https://www.kifid.nl/judgement/uitspraak-2020-617/

- Cruciaal bij deze fraude is dat mensen door het echte telefoonnummer van de alarmlijn van de bank worden gebeld, waardoor het vertrouwen van mensen gewekt wordt en deze fraude plaats kan vinden. Gedupeerden vinden dat de bank meer zou moeten doen om het telefoonnummer te beschermen zodat dit niet zou kunnen gebeuren. Wat is de reactie van ABN Amro daarop? Allereerst een correctie op de vraag: Het *lijkt* dat de klant wordt gebeld door het echte nummer van de bank, maar dat is niet zo. Via een technische truc verschijnt het nummer van de bank in beeld, maar in werkelijkheid wordt er met een ander nummer gebeld. ABN AMRO wil haar klanten beschermen en voorlichten over de risico's die zij lopen. Klanten kunnen van ons verwachten dat wij proberen valse websites/e-mails uit de lucht te halen, we proberen gestolen geld terug te halen, we heffen rekeningen van oplichters op, we proberen frauduleuze betalingen te herkennen, we informatie geven over veilig bankieren, ook samen met andere banken. Helaas kunnen wij niet alle technische trucs uitbannen die bestaan of bedacht worden door criminelen om zich voor te doen als de bank. Daarom zeggen wij altijd tegen klanten dat wij nooit om beveiligingscodes vragen, wij nooit vragen om geld over te boeken, wij nooit linkjes sturen om direct in te loggen in Mobiel of Internet Bankieren. En wij vragen klanten om verdachte gesprekken direct aan ons te melden.

- De te naam stelling van een tegenrekening kan een codewoord zijn met letters en cijfers die geen daadwerkelijke naam vormen. Toch kan een overboeking plaatsvinden, waardoor het verhaal van de oplichter over het overmaken naar een kluisrekening doorgang kan vinden, ook op het afschrift komt de ingevulde code te staan en niet de daadwerkelijke naam van de eigenaar/katvanger van de tegenrekening. Wat is de reactie van ABN Amro daarop? De juistheid of onjuistheid van de naam van de begunstigde mag wettelijk voor de bank geen belemmering zijn voor het uitvoeren van de transactie. (er worden nog steeds veel schrijffouten gemaakt in namen van begunstigden. Als al die transacties automatisch zouden worden geblokkeerd dan hebben we weer een ander probleem). Alleen het juiste rekeningnummer is vereist. Wel geven wij tijdens de overboeking aan dat de combinatie van een naam en een rekeningnummer wel/niet bij elkaar herkend worden door onze systemen. Als het systeem de combinatie niet herkend, dan verschijnt er een melding en het verzoek of de klant de overboeking nog steeds wil uitvoeren. Zie: https://www.abnamro.nl/nl/prive/betalen/iban-naam-check.html Om de transactie door te zetten, moet de klant ervoor kiezen om onze melding te negeren.