reactie ING:

Reactie ING
Voordat we op de vragen ingaan, willen we allereerst benadrukken dat we het erg vinden dat de heer Van Rij en (..,red.) en in 2017 slachtoffer zijn geworden van helpdeskfraude. Wij realiseren ons dat het voor hen een ingrijpende en impactvolle gebeurtenis moet zijn. Omdat mevrouw heeft aangegeven anoniem te willen blijven, zullen we haar niet bij naam noemen en spreken over 'de heer Van Rij en (…, red.)' in onze reactie als we persoonsnamen aanhalen.

Wat is de reactie van ING op deze casus?
De afgelopen jaren, en ook recent nog in april 2021, is veelvuldig contact geweest met de heer Van Rij en (…,red.) over de zaak zelf. Daarbij is de interne klachtenprocedure binnen ING doorlopen en is de zaak door de heer Van Rij en (…,red.) voorgelegd aan het Klachteninstituut Financiële Dienstverlening (Kifid). De Geschillencommissie Financiële Dienstverlening van het Kifid heeft in 2020 de vordering van de heer Van Rij en (…,red.) afgewezen. Het Kifid heeft de zienswijze van ING bevestigd, wat betekent dat ING de schade niet hoeft te vergoeden.

ING heeft uit veiligheidsoverwegingen de wachttijd voor de daglimiet inmiddels aangepast naar 4 uur, deze klant is de dupe van het oude systeem waardoor 30.000 euro kon kwijtraken in plaats van 5.000 euro in de huidige situatie. Gaat ING het verschil in schade vergoeden?
Of een klant in aanmerking komt voor een schadevergoeding beoordelen wij van geval tot geval. Nogmaals, wij vinden het vervelend dat de heer Van Rij en (…,red.) slachtoffer zijn geworden van deze vorm van oplichting, maar wij zullen de schade van de heer Van Rij en (…,red.) niet vergoeden, zoals we hen eerder hebben laten weten. Het Kifid heeft de zienswijze van ING bevestigd.

De heer Van Rij en (…,red.) geven bij Kassa aan dat het verhogen van de wachttijd voor een limietverhoging, zoals doorgevoerd in november 2020, in hun situatie in 2017 had geleid tot een minder hoge schade in 2017. Belangrijk punt bij deze vorm van oplichting is echter dat de klant de volledige toegang en besturing tot zijn computer aan een onbekende derde partij geeft (https://www.ing.nl/de-ing/veilig-bankieren/belangrijke-mededelingen/Helpdeskfraude.html en https://www.politie.nl/themas/helpdeskfraude.html). Vaak zijn het bellers die (gebroken) Engels spreken. De zogenaamde medewerker dringt aan op snelle maatregelen om het bestaande probleem te verhelpen en grote(re) problemen te voorkomen. De crimineel is bereid om tegen betaling de zogenaamde problemen te verhelpen. De heer Van Rij en zijn partner zijn dus slachtoffer geworden van gewiekste oplichters waardoor de schade is ontstaan. Deze oplichters hebben de computer van mevrouw overgenomen. Een langere wachttijd om een limiet te verhogen had de door hen geleden schade ons inziens niet verminderd.

Microsoft omschrijft op haar eigen website wat er vaak gebeurt bij Microsoft fraude (https://pulse.microsoft.com/nl-nl/making-a-difference-nl-nl/na/fa2-5-tips-tegen-telefonische-oplichting-en-phishing/), namelijk:

- Criminelen willen je schadelijke software op je computer laten installeren. Bijvoorbeeld om je wachtwoorden voor internetbankieren te stelen.
- Criminelen willen dat je ze toegang geeft tot je computer, zodat ze mee kunnen kijken en zelf privacygevoelige gegevens stelen.
- Criminelen willen je een valse transactie met je creditcardgegevens laten doen of geld ontfutselen.
- Criminelen willen je naar frauduleuze websites lokken, om je daar privacygevoelige informatie in te laten voeren, die ze vervolgens kunnen gebruiken

Wij verwijzen je graag naar Microsoft voor hun reactie op deze vorm van niet-bancaire fraude waarbij hun naam wordt misbruikt.