**Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2022-0021**
**(mr. F.H.E. Boerma, voorzitter en mr. P. Meijer, secretaris)**

| | |
|---|---|
| Klacht ontvangen op | : 17 februari 2021 |
| Ingediend door | : De consumenten |
| Tegen | : ING Bank N.V., gevestigd te Amsterdam, verder te noemen de bank |
| Datum uitspraak | : 12 januari 2022 |
| Aard uitspraak | : Niet-bindend advies |
| Uitkomst | : Vordering gedeeltelijk toegewezen |
| Bijlage | : Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden |

## Samenvatting

Niet-toegestane betalingstransacties. De consumenten zijn op 28 juli 2020 slachtoffer geworden van fraude. Op 29 juni 2020 is een Mobiel Bankieren App op een telefoon van een onbekend gebleven derde toegevoegd aan het account van de consumenten. Via deze Mobiel Bankieren App zijn drie frauduleuze betalingstransacties goedgekeurd. De consumenten vorderen van de bank vergoeding van deze niet-toegestane transacties. De bank stelt zich op het standpunt dat de schade voor rekening van de consumenten dient te blijven, omdat de consumenten niet voldaan hebben aan hun verzwaarde stelplicht en het volgens de bank niet anders kan dan dat zij met grove nalatigheid hebben gehandeld. De commissie is van mening dat de consumenten wel hebben voldaan aan hun verzwaarde stelplicht en niet is komen vast te staan dat zij met grove nalatigheid gehandeld hebben. De vordering van de consumenten wordt (grotendeels) toegewezen.

## 1. De procedure

1.1 De commissie beslist op basis van haar reglement en op basis van de door partijen aan Kifid ingestuurde documenten inclusief bijlagen. Het gaat om: 1) het klachtformulier van de consumenten; 2) de aanvullende stukken van de consumenten; 3) het verweerschrift van de bank;

1.2 Partijen zijn opgeroepen voor een hoorzitting op 1 november 2021. Op de hoorzitting waren de consumenten aanwezig. De bank nam via een videoverbinding deel aan de hoorzitting.

1.3 De consumenten hebben gekozen voor een niet-bindend advies. Dit betekent dat partijen elkaar niet aan de uitspraak kunnen houden.

## 2. Het geschil

*Wat is er gebeurd?*

2.1 De consumenten houden bij de bank een betaalrekening met bijbehorende betaalpas en pincode aan. De consumenten maken gebruik van internetbankieren en (enige tijd) de Mobiel Bankieren App van de bank. Op deze overeenkomst is de "Brochure voorwaarden en overige regelingen voor particuliere rekeninghouders" (verder: de brochure), van toepassing. De tekst van de relevante artikelen uit de brochure is in de bijlage opgenomen.

2.2 Op 29 juni 2020 is er een Mobiel Bankieren App (geïnstalleerd op een OnePlus 5 telefoon) aan het account van de consumenten gekoppeld. Vervolgens is er via deze Mobiel Bankieren App in de periode tussen 29 juni 2020 en 28 juli 2020 tientallen keren ingelogd op het account van de consumenten, zonder dat er transacties verricht zijn. Op 28 juli 2020 zijn er bedragen van € 100,81, € 336,67 en € 1.980,71 overgeboekt van de betaalrekening van de consumenten naar een rekening bij ABN AMRO Bank. De betalingen zijn ingevoerd via internetbankieren, vanaf een computer en IP-adres niet eerder gebruikt voor het inloggen op het account van de consumenten, en bevestigd door middel van de eerder genoemde Mobiel Bankieren App. De omschrijving vermeld bij de transacties is "Politie Zorgpolis". De tegenrekening is echter niet van de zorgverzekeraar van de consumenten. De consumenten betwisten deze transacties verricht te hebben, of hiervoor toestemming verleend te hebben.

2.3 Een vierde transactie van € 1.992,06 naar dezelfde rekening bij ABN AMRO Bank is door de bank geblokkeerd. Door ABN AMRO Bank is een bedrag van € 58,19 veiliggesteld en op 25 september 2020 teruggeboekt naar de rekening van de consumenten.

*De klacht en vordering*

2.4 De consumenten klagen over het feit dat de bank zonder hun toestemming drie bedragen van hun rekening heeft overgeschreven naar de rekening van een onbekende derde. Hierdoor lijden de consumenten schade, waarvoor de consumenten gecompenseerd willen worden door de bank. De consumenten vorderen een bedrag van € 2.418,19 van de bank.

2.5 De consumenten zijn van mening dat zij zich gehouden hebben aan de regels voor veilig bankieren en hen niets verweten kan worden. Zo hebben de consumenten nimmer hun gebruikersnaam, wachtwoord, geboortedatum, pasnummer en/of pasvervaldatum aan derden beschikbaar gesteld. Ook hebben zij niet op links in verdachte e-mails geklikt. Voorafgaand aan de fraude zijn de consumenten wel drie keer benaderd door fraudeurs/oplichters (onder andere via telefoon en whatsapp), maar elke keer hebben de consumenten goed opgelet en geen gegevens prijsgegeven. Van de laatste fraudepoging is ook melding gedaan bij de bank.

2.6 De consumenten benadrukken dat zij geen OnePlus 5 telefoon bezitten. Op 29 juni 2020, de dag waarop de frauduleuze koppeling van de Mobiel Bankieren App op de OnePlus 5 telefoon aan het account van de consumenten heeft plaatsgevonden, zijn de consumenten naar het (toenmalig) regiokantoor van ING te [plaats] gegaan voor support bij het installeren van een Mobiel Bankieren App op een telefoon (IPhone) van de consumenten. De consumenten hebben hun inloggegevens niet afgegeven aan de ING-medewerker die hen hielp, maar zij hebben wel ingelogd met hun gebruikersnaam en wachtwoord op een computer van het ING-kantoor. De ING-medewerker heeft de bankpas van de consumenten ook gezien. Uiteindelijk is de Mobiel Bankieren App die dag niet geïnstalleerd op de telefoon van de consumenten, maar werd hen geadviseerd om een scanner te gebruiken. Achteraf gezien kan het volgens de consumenten niet anders dan dat de frauduleuze koppeling van de Mobiel Bankieren App aan het account van de consumenten bij het ING-kantoor te [plaats] tot stand is gekomen.

*Het verweer*

2.7 De bank heeft de volgende verweren gevoerd. Zoals in de Uniforme Veiligheidsregels (pagina 40 van de brochure) staat vermeld onder het kopje "Wat moet u doen" dient de klant zijn of haar beveiligingscodes geheim te houden en te zorgen voor een goede beveiliging van de apparatuur die wordt gebruikt voor bankzaken. Onder het kopje "Toelichting veiligheids-regels" staat vermeld dat niet alleen de pincode die bij een bankpas wordt gebruikt een beveiligingscode is, maar ook de codes die worden gebruikt voor de Mobiel Bankieren App (de vijf cijferige Mobiele pincode). Daarnaast staat in de Uniforme Veiligheidsegels (onder punt 3, pagina 41 van de brochure) dat apparatuur die wordt gebruikt voor bankzaken dient te zijn beveiligd met een toegangscode en dat dient te worden uitgelogd als men klaar is met het regelen van bankzaken.

2.8 Op grond van artikel 15.1. van de Voorwaarden Betaalrekening (pagina 20 van de brochure) is de Mobiel Bankieren App een betaalinstrument. Op grond van artikel 16.1. (pagina 20 van de brochure) dient de Mobiele pincode van de Mobiel Bankieren App geheim te worden gehouden. Op grond van artikel 59.2. van de Voorwaarden Betaalrekening (pagina 26 van de brochure) vergoedt ING de schade als gevolg van misbruik van betaalartikelen niet, indien sprake is van grove nalatigheid. Daar is sprake van indien de klant niet heeft voldaan aan de verplichtingen die horen bij het gebruik van betaalinstrumenten.

2.9 Op 29 juni 2020 is er een Mobiel Bankieren App aan het account van de consumenten gekoppeld. De betwiste betalingen van 28 juli 2020 zij ingevoerd via een computer met Windows 10 als besturingssysteem, waarna de autorisatie is uitgevoerd via de op 29 juni 2020 toegevoegde Mobiel Bankieren App.

De consumenten hebben volgens de bank nagelaten een verklaring te verstrekken voor het feit dat derden kennelijk over een aantal gegevens van hen hebben kunnen beschikken, benodigd voor het tot stand brengen van de koppeling van de Mobiel Bankieren App aan het account van consumenten. Zo is onder andere een TAN code, welke code via sms naar de telefoon van de consumenten is verstuurd, vereist voor het activeren van de Mobiel Bankieren App.

2.10 De Bank stelt dat er in haar systeem geen contactmoment met de consumenten op 29 juni 2020 is vastgelegd. Wel zijn er contactmomenten terug te vinden op 10 en 16 juni 2020.

2.11 Omdat volgens de bank niet duidelijk is geworden hoe derden over de benodigde gegevens konden beschikken om een Mobiel Bankieren App aan het account van de consumenten te koppelen, wordt de bank onvoldoende in de gelegenheid gesteld te toetsen of de consumenten zich in voldoende mate aan de geldende voorwaarden en veiligheidsinstructies hebben gehouden. Volgens de bank kan het niet anders dan dat de consumenten grof nalatig gehandeld hebben. Dit leidt er volgens de bank toe dat de schade niet voor vergoeding in aanmerking komt. De bank verwijst hierbij naar eerdere jurisprudentie van de geschillencommissie van Kifid, waaronder Geschillencommissie Kifid nr. 2020-1055.[1]

## 3. De beoordeling

3.1 Aan de commissie ligt de vraag voor of de bank de schade van € 2.418,19 die de consumenten stellen te hebben geleden, aan de consumenten moet vergoeden. De commissie is van oordeel dat de bank een bedrag van € 2.360,- dient te vergoeden en licht hieronder toe waarom.

*Wat is het toetsingskader?*

3.2 De consumenten hebben het standpunt ingenomen dat de bank de overboekingen zonder hun instemming heeft uitgevoerd. Bij het ontbreken van een dergelijke instemming wordt een betalingstransactie overeenkomstig artikel 7:522 lid 2 laatste volzin van het Burgerlijk Wetboek (hierna: BW) als 'niet toegestaan' aangemerkt. Op grond van artikel 7:528 lid 1 BW moet de bank in geval van een niet-toegestane betalingstransactie de consument onmiddellijk het bedrag van de niet-toegestane betalingstransactie terugbetalen. Volgens artikel 7:529 lid 1 BW draagt de betaler echter alle verliezen die uit niet-toegestane betalingstransacties voortvloeien, indien deze zich hebben voorgedaan doordat hij of zij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen.

[1] Te vinden op www.kifid.nl

Zo is een betaaldienstgebruiker ingevolge artikel 7:524 lid 2 BW verplicht alle redelijke maatregelen te treffen om de veiligheid van de gepersonaliseerde veiligheidskenmerken van een betaalinstrument te waarborgen.

*Verzwaarde stelplicht*

3.3 De bank stelt dat de consumenten met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW dan wel de verplichtingen voortvloeiende uit de brochure niet zijn nagekomen. Alhoewel het aan de bank is om te bewijzen dat sprake is van grove nalatigheid door de consumenten, rust op de consumenten een 'verzwaarde stelplicht'.[2] Dat betekent dat de consumenten tenminste enig inzicht dienen te geven in de wijze waarop hun inloggegevens in onbevoegde handen zouden kunnen zijn geraakt (waardoor er op het account van de consumenten ingelogd kon worden en de Mobiel Bankieren App aan het account van de consumenten gekoppeld kon worden), zodat de bank zich daarover een beeld kan vormen. Een andere regel zou de bank voor onaanvaardbare risico's van misbruik plaatsen.[3] Dat betekent dat van de consumenten kan worden verwacht dat zij zo goed mogelijk een verklaring moeten bieden voor de omstandigheid dat hun gegevens kennelijk bij derden bekend zijn geraakt.

3.4 De bank stelt zich op het standpunt dat de consumenten geen verklaring geven voor het feit dat hun gegevens bekend geraakt zijn bij derden waardoor deze derden de drie frauduleuze overboekingen hebben kunnen doen. Met andere woorden: de consumenten zouden niet hebben voldaan aan hun verzwaarde stelplicht. Volgens de bank kan het niet anders zijn dan dat de consumenten op enig moment hun inloggegevens aan derden ter beschikking hebben gesteld en daarmee met grove nalatigheid hun verplichtingen uit hoofde van artikel 7:524 BW dan wel hun verplichtingen uit de brochure niet zijn nagekomen. De commissie gaat niet mee in dit standpunt van de bank.

3.5 De commissie is van mening dat de consumenten wel enig inzicht gegeven hebben in de wijze waarop hun inloggegevens in onbevoegde handen geraakt zouden kunnen zijn. De consumenten hebben immers aangegeven dat zij op de dag waarop de frauduleuze koppeling van de Mobiel Bankieren App op de OnePlus 5 telefoon heeft plaatsgevonden, bij een ING-kantoor langs geweest zijn, waarbij zij hebben ingelogd op hun account, hetgeen nodig was voor het installeren van de Mobiel Bankieren App. Hierbij is de bankpas zichtbaar geweest voor de bankmedewerker. Volgens de consumenten kan het niet anders dan dat de frauduleuze koppeling van de Mobiel Bankieren App aan het account van de consumenten bij het ING-kantoor te Harderberg tot stand is gekomen.

---

[2] Zie o.a. Geschillencommissie Kifid nrs. 2019-308, 2019-733, 2020-853 en 2020-1055, te vinden op www.kifid.nl

[3] Zie Geschillencommissie Kifid nrs. 2014-144 en 2019-733, te vinden op www.kifid.nl

Hoewel de door de consumenten geschetste gang van zaken niet is komen vast te staan, hebben zij hiermee wel enig inzicht gegeven in de wijze waarop hun inloggegevens in onbevoegde handen geraakt *kunnen* zijn, waardoor de bank zich hierover een beeld heeft kunnen vormen. De consumenten, op leeftijd, zijn hierover tijdens de zitting ook bevraagd en maakten een betrouwbare indruk. De commissie heeft daardoor ook niet het beeld gekregen dat de consumenten zomaar wat vertellen. De commissie is overigens niet gebleken dat de bank nader onderzoek gedaan heeft naar de verklaring van de consumenten, anders dan het bekijken van in de bankadministratie geregistreerde contactmomenten.

3.6 De commissie benadrukt verder dat het hier een atypisch fraudegeval betreft. Uit de loggegevens die de bank heeft overgelegd blijkt dat, nadat de Mobiel Bankieren App op 29 juni 2020 op de OnePlus 5 telefoon gekoppeld is aan het account van de consumenten, er via deze Mobiel Bankieren App in de periode tussen 29 juni 2020 en 28 juli 2020 tientallen keren is ingelogd op het account van de consumenten, zonder dat er transacties verricht zijn. Pas na een maand na de koppeling van de Mobiel Bankieren App aan het account van de consumenten vinden de frauduleuze transacties plaats. Dit tijdsverloop is erg opvallend. In dit soort fraudegevallen wordt doorgaans direct geld opgenomen/gepoogd geld op te nemen van de rekening, omdat de kans op ontdekking groter wordt naarmate de tijd verstrijkt. Ook de “maskering” van de betalingen als zijnde betalingen aan de zorgverzekeraar van de consumenten is opvallend te noemen.

3.7 Tot slot ziet de commissie geen aanwijzingen dat de consumenten onzorgvuldig of lichtzinnig zijn omgegaan met hun pas en inloggegevens, dan wel dat zij op andere wijze met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW dan wel de verplichtingen voortvloeiende uit de brochure niet zijn nagekomen. De commissie krijgt juist de indruk dat de consumenten erg voorzichtig zijn en de meeste oplichtingstrucs waar vooral veel ouderen tegenwoordig slachtoffer van worden doorzien. Hierbij merkt de commissie op dat het feit dat de consumenten op het bankfiliaal hebben ingelogd op hun account (zonder daarbij hun inloggegevens mede te delen aan de bankmedewerker), waarbij zij mogelijk ook een TAN-code hebben ontvangen en ingevoerd en het feit dat hun pas zichtbaar of misschien zelfs in handen van de bankmedewerker geweest is, niet maakt dat de consumenten met grove nalatigheid gehandeld hebben. De consumenten hebben hun inloggegevens immers niet (bewust) prijsgegeven aan zomaar een derde en zij verkeerden in de veronderstelling dat zij door een te vertrouwen bankmedewerker geholpen werden bij het installeren van een Mobiel Bankieren App op hun eigen telefoon. Het zou om die reden niet redelijk zijn de consumenten te verwijten dat ze dat vertrouwen niet hadden mogen hebben.

3.8 Gelet op al het bovenstaande is de commissie van mening dat de feiten en omstandigheden in deze zaak anders zijn dan in de door de bank aangehaalde jurisprudentie van de geschillencommissie van Kifid en de bank meer moet stellen dan dat "het niet anders kan dan" dat de consumenten met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW dan wel de verplichtingen voortvloeiende uit de brochure niet zijn nagekomen. Nu de bank geen aanvullende feiten en/of omstandigheden heeft aangedragen waaruit de "grove nalatigheid" van de consumenten blijkt, acht de commissie de klacht van de consumenten gegrond en oordeelt dat de bank gehouden is de betwiste transacties aan de consumenten te vergoeden. Nu de ABN AMRO Bank een bedrag van € 58,19 heeft veiliggesteld en aan de consumenten heeft geretourneerd, wijst de commissie de vordering van de consumenten toe, min het al door de ABN AMRO betaalde, dus tot een bedrag van € 2.360,-.

## 4. De beslissing

De commissie beslist dat de bank een bedrag van € 2.360,- aan de consumenten vergoedt binnen vier weken nadat deze beslissing aan partijen is verstuurd.

*Deze uitspraak is een niet-bindend advies. Tegen deze uitspraak staat geen hoger beroep open bij de Commissie van Beroep Financiële Dienstverlening. U kunt de zaak nog wel aan de rechter voorleggen.*

*Binnen twee weken na de verzenddatum van deze uitspraak kunt u een schriftelijk verzoek indienen tot herstel van vergissingen in de uitspraak zoals schrijffouten, een verkeerde naam/datum of rekenfouten. De beslissing van de geschillencommissie in de uitspraak kan hiermee niet ter discussie worden gesteld. Binnen een maand na de verzenddatum van de uitspraak kunt u een schriftelijk verzoek indienen om de uitspraak aan te vullen als u vindt dat de geschillencommissie niet heeft beslist over alle onderdelen van uw vordering. Dit ziet niet op de situatie waarin u meent dat de geschillencommissie in haar uitspraak niet uitdrukkelijk al uw argumenten, ter onderbouwing van uw vordering, heeft behandeld. Meer informatie hierover staat in artikel 40 van het reglement van de geschillencommissie, te vinden op de website www.kifid.nl/reglementen-en-statuten.*

## Bijlage - Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

### *Burgerlijk Wetboek*

*Artikel 7:522*
*1.Een betaaldienstverlener voert een betalingstransactie slechts uit met instemming van de betaler met de uitvoering van de betaalopdracht.*
*2.De instemming met een betaalopdracht wordt verleend overeenkomstig de tussen de betaler en zijn betaaldienstverlener overeengekomen vorm en procedure. Bij gebreke van een dergelijke instemming wordt een betalingstransactie als niet toegestaan aangemerkt.*
*(…)*

*Artikel 7:524*
*1.De betaaldienstgebruiker die gemachtigd is om een betaalinstrument te gebruiken,*
*a. gebruikt het betaalinstrument overeenkomstig de voorwaarden die op de uitgifte en het gebruik van het betaalinstrument van toepassing zijn, en*
*b. stelt de betaaldienstverlener, of de door laatstgenoemde gespecificeerde entiteit, onverwijld in kennis van het verlies, de diefstal of onrechtmatig gebruik van het betaalinstrument of van het niet-toegestane gebruik ervan.*
*2.Voor de toepassing van het eerste lid, onder a, neemt de betaaldienstgebruiker, zodra hij een betaalinstrument ontvangt, in het bijzonder alle redelijke maatregelen om de veiligheid van de gepersonaliseerde veiligheidskenmerken ervan te waarborgen.*

*Artikel 7:528*
*1.Onverminderd artikel 526, betaalt de betaaldienstverlener van de betaler, in geval van een niet-toegestane betalingstransactie, onmiddellijk het bedrag van de niet-toegestane betalingstransactie terug en herstelt hij, in voorkomend geval, de betaalrekening die met dat bedrag was gedebiteerd, in de toestand zoals die geweest zou zijn, indien de niet-toegestane betalingstransactie niet zou hebben plaatsgevonden.*
*(…)*

*Artikel 7:529*
*1.In afwijking van artikel 528 draagt de betaler tot een bedrag van ten hoogste € 150 het verlies met betrekking tot niet-toegestane betalingstransacties dat voortvloeit uit het gebruik van een verloren of gestolen betaalinstrument of, indien de betaler heeft nagelaten de veiligheid van de gepersonaliseerde veiligheidskenmerken ervan te waarborgen, uit onrechtmatig gebruik van een betaalinstrument.*
*2.De betaler draagt alle verliezen die uit niet-toegestane betalingstransacties voortvloeien, indien deze zich hebben voorgedaan doordat hij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 524 niet is nagekomen. In dergelijke gevallen is het in het eerste lid bedoelde maximumbedrag niet van toepassing.*

*3.In gevallen waarin de betaler, zonder frauduleus of opzettelijk te hebben gehandeld, zijn verplichtingen uit hoofde van artikel 524 niet is nagekomen, kan de rechter de in het eerste en tweede lid van dit artikel bedoelde aansprakelijkheid beperken, met name rekening houdend met de aard van de gepersonaliseerde veiligheidskenmerken van het betaalinstrument en met de omstandigheden waarin het is verloren, gestolen of onrechtmatig gebruikt.*
*(…)*

***Brochure Voorwaarden en overige regelingen voor particuliere rekeninghouders***

*Voorwaarden betaalrekening*

*15.1 Als rekeninghouder kunt u met uw Betaalrekening gebruik maken van de betaaldiensten van ING, zoals geld overmaken, storten, ontvangen, opnemen en Incasso. Daarbij maakt u gebruik van betaalinstrumenten zoals de Betaalpas, Overschrijvingskaarten, Mijn ING, de Mobiel Bankieren App en de Saldolijn.*

*16.1 Bij een betaalinstrument horen vaak gepersonaliseerde veiligheidskenmerken. Bijvoorbeeld een inlognaam, een wachtwoord, een pincode. Deze mogen alleen door u persoonlijk worden gebruikt. Houd deze geheim en neem alle denkbare maatregelen om fraude en misbruik te voorkomen.*
*16.2 ING geeft u via ing.nl en de productvoorwaarden instructies over hoe u veilig om moet gaan met gepersonaliseerde veiligheidskenmerken en betaalinstrumenten. Deze instructies moet u opvolgen.*
*16.3 ING geeft u actuele informatie over maatregelen die u moet nemen om fraude en ander misbruik te voorkomen. Hiervan moet u maandelijks kennisnemen en u moet ernaar handelen.*

*Overige voorwaarden*

*59.2 ING betaalt niets terug als er van uw kant sprake is van fraude, opzet of grove nalatigheid. U heeft dan niet aan de verplichtingen voldaan die horen bij het gebruik van uw betaalinstrument.*

*Uniforme veiligheidsregels*
*(…)*

*Toelichting veiligheidsregels*
*1. Houd uw beveiligingscodes geheim*.*
*(…)*

*Denk hierbij aan het volgende:*
*• Beveiligingscodes zijn niet alleen de pincode die u in combinatie met de bankpas gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronische betalingen te doen en/of gebruik te maken van internetbankieren en mobiele bank apps:*
*- Wachtwoord*
*- SMS-codes*
*- Activeringscode*
*- Bevestigingscode*
*- Pincode (betaalpas, creditcard, mobiele pas, ING Scanner)*
*- Mobiele pincode*
*- ING Scanner: kleurencode en code*
*(…)*

*3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.*
*Denk hierbij aan het volgende:*
*• Zorg dat de geïnstalleerde software op de apparatuur, zoals computer, tablet en/of smartphone, die u voor het regelen van uw bankzaken gebruikt, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals virusscanner en firewall;*
*• Installeer geen illegale software;*
*• Beveilig de toegang tot de apparatuur die u gebruikt voor het regelen van uw bankzaken met een toegangscode.*
*• Zorg er daarnaast voor dat door ING verstrekte toepassingen op de apparatuur die u gebruikt voor het regelen van uw bankzaken niet door onbevoegden kunnen worden gebruikt;*
*• Log altijd uit als u klaar bent met het regelen van uw bankzaken.*