

## UNIFORME VEILIGHEIDSREGELS PARTICULIEREN

*[Instructie voor de bank: Dit document geeft beide versies (bijlage 1 en 2 van 19.003\_LB\_NL) van de Uniforme veiligheidsregels particulariseren geïntegreerd weer, en is enkel bedoeld om inzichtelijk te maken wat de verschillen tussen beide versies zijn.]*

### Waarover gaan deze regels?

Elektronisch bankieren en elektronisch betalen moeten veilig zijn. Denk aan het regelen van uw dagelijkse bankzaken via internetbankieren en/of mobiele bank apps, het betalen bij betaalautomaten in winkels en het opnemen van geld bij de geldautomaat. De bank heeft hierin een belangrijke taak, maar u ook. Wat u moet doen, vindt u in deze veiligheidsregels.

### Waarom is het belangrijk dat u zich houdt aan deze regels?

U vermindert de kans dat u het slachtoffer wordt van fraudeurs sterk als u de regels opvolgt. Het is voor consumenten wettelijk geregeld dat een bedrag, dat zonder uw toestemming van uw betaalrekening is afgeschreven, door de bank wordt vergoed. De bank is echter niet altijd verplicht dat bedrag aan u te vergoeden. Wanneer u zich aan de onderstaande vijf veiligheidsregels houdt, loopt u niet het risico dat de gehele schade voor uw eigen rekening komt.

### Wat moet u doen?

#### ❶ Houd uw beveiligingscodes geheim [\*].

*[Instructie voor de bank: Let op, de asterix (\*) achter veiligheidsregel 1 dient **niet** te worden weergegeven door banken die, voor betaalinitiatie- en rekeninginformatiedienstverleners, een zogeheten 'dedicated interface' met redirection-mechanisme naar de eigen online bankomgeving aanbieden én daarmee bovendien door DNB zijn uitgezonderd van de wettelijke verplichting om een zogeheten 'fall-back' in te richten. Andere banken – hier: banken die géén dedicated interface met een redirection-mechanisme naar de eigen online bankomgeving aanbieden, én banken die dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten – moeten de asterix (\*) wel achter veiligheidsregel 1 vermelden.]*

#### ❷ Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.

#### ❸ Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.

#### ❹ Controleer uw bankrekening.

#### ❺ Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.

Elk van deze veiligheidsregels worden hieronder toegelicht.

## Toelichting veiligheidsregels

### 1 Houd uw beveiligingscodes geheim [\*].

[\*] [Banken die géén 'dedicated interface' met een redirection-mechanisme naar de eigen online bankomgeving aanbieden én banken die dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een 'fall-back' in te richten, geven hier (omkaderd) het volgende weer:]

\* Door gewijzigde wetgeving kunnen andere financiële dienstverleners u een nieuw soort diensten aanbieden. Daarmee kunt u bijvoorbeeld meer overzicht over uw financiën krijgen (rekeninginformatiediensten) of uw online aankopen afrekenen (betalinitiatiediensten). Om die diensten te kunnen verlenen, moeten deze derde dienstverleners zijn ingeschreven in de openbare registers [klik [hier](#)] van De Nederlandsche Bank (DNB). Als u gebruik maakt van een rekeninginformatie- en/of betaalinitiatiedienst van een dergelijke derde dienstverlener, geeft u die partij toegang tot uw betaalrekening om een betaling op te starten (bij een betaalinitiatiedienst) of rekeninginformatie op te halen (bij een rekeninginformatiedienst). Overigens kan ook [naam eigen bank] zelf u betaalinitiatie- en/of rekeninginformatiediensten aanbieden met betrekking tot betaalrekeningen die u mogelijk bij andere banken aanhoudt.

[Instructie voor de bank: Een betaalrekeninghouder kan in bepaalde gevallen de via zijn bank ontvangen beveiligingscodes voor online bankieren, invoeren op de website of app van een derde dienstverlener, als de betaalrekeninghouder gebruik wil maken van de betaalinitiatie- en/of rekeninginformatiedienst die deze derde dienstverlener aanbiedt. Hier per bank aangeven hoe de klant, als deze gebruik wil maken van een rekeninginformatie- en/of betaalinitiatiedienst van een geautoriseerde derde dienstverlener, dient om te gaan met de van de bank ontvangen veiligheidscodes om in te loggen in, en betalingen te autoriseren via, het internetbankieren en/of de mobiele bankapp van zijn bank. Aangeven of – en zo ja, in welke gevallen – de klant die veiligheidscodes mag invoeren op de website of app van de derde dienstverlener.]

Denk hierbij aan het volgende:

- [Instructie voor de bank: Onderstaande zin wordt alleen weergegeven door banken die, voor betaalinitiatie- en rekeninginformatiedienstverleners, een 'dedicated interface' met redirection-mechanisme naar de online bankomgeving aanbieden én daarmee bovendien door DNB zijn uitgezonderd van de wettelijke verplichting om een 'fall-back' in te richten. Banken die géén dedicated interface met een redirection-mechanisme naar de eigen online bankomgeving aanbieden én banken dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten, laten de onderstaande zin achterwege.]

[Zorg ervoor dat beveiligingscodes nooit aan een ander bekend kunnen worden;]

- 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. Dat kunnen bijvoorbeeld de codes zijn die een door de bank verstrekte codecalculator aangeeft, codes die u via een mobiele bank app en/of codes die u per SMS van uw bank ontvangt.

[Instructie voor de bank: Verwijzen naar bankspecifieke authenticatie en autorisatieprocedure.];

- [Instructie voor de bank: Onderstaande zin wordt alleen weergegeven door banken die, voor betaalinitiatie- en rekeninginformatiedienstverleners, een 'dedicated interface' met redirection-mechanisme naar de eigen online bankomgeving aanbieden én bovendien daarmee door DNB zijn uitgezonderd van de wettelijke verplichting om een 'fall-back' in te richten. Banken die géén dedicated interface met een redirection-mechanisme naar de eigen online bankomgeving aanbieden én banken dat op zich wel aanbieden, maar

*niet door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten, laten de onderstaande zin achterwege.].*

[U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die de bank aangeeft.] *[Instructie voor de bank: Per bank verwijzen naar vindplaats met informatie op welke manier beveiligingscodes gebruikt mogen worden.];*

- Schrijf of sla de codes niet op. Of, als het echt niet anders kan, alleen in een voor anderen onherkenbare vorm die alleen door uzelf is te ontcijferen. Bewaar in dat geval de versleutelde informatie niet bij uw bankpas of bij apparatuur waarmee u uw bankzaken regelt;
- Als u zelf een beveiligingscode kunt kiezen, zorg dan dat die niet gemakkelijk te raden is. Kies bijvoorbeeld geen geboortjaar, naam van een familielid of postcode;
- Zorg ervoor dat niemand kan meekijken als u uw beveiligingscodes intikt. Het gaat hier niet alleen om uw pincode, maar ook om alle andere codes die u moet gebruiken om elektronische betalingen te doen en/of gebruik te maken van internetbankieren en mobiele bank apps;
- Geef nooit een beveiligingscode door per telefoon, e-mail of op een andere wijze dan de bank u heeft voorgeschreven. *[Instructie voor de bank: Per bank verwijzen naar vindplaats met informatie op welke manier beveiligingscodes gebruikt mogen worden.] [Banken die, voor betaaliniciatie- en rekeninginformatiedienstverleners, een 'dedicated interface' met redirection-mechanisme naar de online bankomgeving aanbieden én daarmee bovendien door DNB zijn uitgezonderd van de wettelijke verplichting om een 'fall-back' in te richten, geven vervolgens de volgende zin weer:] [Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank of andere dienstverlener, zoals een computerbeveiligingsbedrijf, te zijn. De bank of andere dienstverleners zullen u op deze wijze **nooit** om beveiligingscodes vragen.] [Instructie voor de bank: Banken die géén dedicated interface met een redirection-mechanisme naar de eigen online bankomgeving aanbieden én banken dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten, geven in plaats daarvan de volgende zin weer:] [Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank te zijn. De bank zal u op deze wijze **nooit** om beveiligingscodes vragen.]*

## ② Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.

*Denk hierbij aan het volgende:*

- Laat u niet afleiden als u de bankpas gebruikt en controleer of u uw eigen bankpas daarna terugkrijgt;
- Berg de bankpas altijd op een veilige plaats op en zorg ervoor dat u hem niet gemakkelijk kunt verliezen. Controleer regelmatig of u de bankpas nog in uw bezit heeft.

## 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 de bank 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.

#### 4 Controleer uw bankrekening.

Controleer altijd zo spoedig mogelijk de van uw bank ontvangen elektronische of papieren rekeninginformatie op eventuele transacties waarvoor u geen toestemming heeft gegeven. Doe dit in ieder geval elke twee weken als de bank voor u elektronische rekeninginformatie ter beschikking stelt. Als u alleen rekeninginformatie op papier ontvangt, controleer deze dan in ieder geval binnen twee weken na ontvangst. Als er schade voor de bank ontstaat doordat het voor u enige tijd onmogelijk is geweest uw rekeninginformatie te controleren, dan kan de bank u vragen aan te tonen dat dit in alle redelijkheid niet mogelijk was.

#### 5 Meld incidenten direct aan de bank en volg aanwijzingen van de bank op.

Denk hierbij aan het volgende:

- Neem in de volgende gevallen in elk geval direct met de bank contact op:
  - u heeft uw bankpas niet meer in uw bezit of weet niet waar deze is;
  - u weet of vermoedt dat iemand anders[, zonder uw toestemming,] uw beveiligingscode kent of heeft gebruikt;  
*[Instructie voor de bank: Het opnemen van de zinsnede ‘, zonder uw toestemming,’ in bovenstaande zin is verplicht voor banken die geen ‘dedicated interface’ met redirection-mechanisme naar de eigen online bankomgeving aanbieden én voor banken dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een ‘fall-back’ in te richten. Banken die wel een dedicated interface met redirection-mechanisme naar de eigen online bankomgeving aanbieden én bovendien daarmee door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten, laten de zinsnede ‘, zonder uw toestemming,’ achterwege.]*
  - u ziet dat er transacties op uw bankrekening hebben plaatsgevonden, waarvoor u geen toestemming heeft gegeven;
  - u heeft uw mobiele apparaat met betaaltoepassing van de bank niet meer, tenzij u dit apparaat aan een ander heeft overgedragen en eerst de betaaltoepassing heeft verwijderd;
- Neem ook direct contact op met de bank als u iets vreemds of ongebruikelijks ervaart bij het elektronisch betalen of het online regelen van uw bankzaken[, zoals een andere manier van inloggen bij uw bank].  
*[Instructie voor de bank: Het opnemen van de zinsnede ‘, zoals een andere manier van inloggen bij uw bank’ in bovenstaande zin is verplicht om voor banken die een ‘dedicated interface’ met redirection-mechanisme naar de eigen online bankomgeving aanbieden én bovendien daarmee door DNB zijn uitgezonderd van de wettelijke verplichting om een ‘fall-back’ in te richten. Banken die geen dedicated interface met redirection-mechanisme naar de eigen online bankomgeving aanbieden én voor banken dat op zich wel aanbieden, maar niet door DNB zijn uitgezonderd van de wettelijke verplichting om een fall-back in te richten, laten de zinsnede ‘, zoals een andere manier van inloggen bij uw bank,’ in bovenstaande zin achterwege.]*

De bank kan zorgen voor een blokkade om (verdere) schade te voorkomen. Als de bank u aanwijzingen geeft, bijvoorbeeld om nieuwe incidenten te voorkomen, dan moet u deze aanwijzingen opvolgen. Ook hierbij zal de bank u **nooit** om beveiligingscodes vragen.