Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2021-0782
(mr. F.H.E. Boerma, voorzitter, mr. M.D.H. Nelemans,
prof. mr. T.H.M. van Wechem, leden en mr. D.W.Y. Sie, secretaris)

Klacht ontvangen op	: 10 maart 2021
Ingediend door	: De consument
Tegen	: ABN AMRO Bank N.V., gevestigd te Amsterdam, verder te noemen de bank
Datum uitspraak	: 2 september 2021
Aard uitspraak	: Bindend advies
Uitkomst	: Vordering afgewezen
Bijlage	: Relevante bepalingen uit wet- en regelgeving

Samenvatting

Klacht over de opname van persoonsgegevens in het Incidentenregister en het Extern Verwijzingsregister. De consument stelt dat haar bankpas is gestolen na een bezoek aan een parfumerie en zij stelt dat haar pincode is gefilmd door de fraudeur. In de daaropvolgende dagen is het (spaar)geld van de consument opgenomen. Vervolgens is er geld afkomstig uit fraude op de betaalrekening van de consument gestort. De commissie is onder meer van oordeel dat de genoemde omstandigheden vallen binnen het (gedrags)patroon van een persoon die zich als geldezel gedraagt. De commissie ziet geen grond om de consument schadevergoeding toe te wijzen. De vordering van de consument wordt afgewezen.

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 consument; 2) het verweerschrift van de bank; 3) de repliek van de consument en 4) de dupliek van de bank.

1.2 Partijen zijn opgeroepen voor een hoorzitting op 5 juli 2021. Op de hoorzitting was de consument aanwezig samen met de heer [naam] (vader). De vertegenwoordiger van de consument mevrouw mr. J.C.M. Maas-Holla (jurist) was telefonisch aanwezig. De bank was eveneens aanwezig. Tijdens de hoorzitting heeft de consument een kopie van haar aanvullende verklaring overgelegd aan de bank en de commissie.

1.3 De consument en de bank hebben gekozen voor een bindend advies. Dit betekent dat partijen elkaar aan de uitspraak kunnen houden.

2. Het geschil

Wat is er gebeurd?

2.1 De consument hield tot enig moment een betaalrekening en spaarrekening aan bij de bank.

2.2 Op 23 juli 2020 om 16:26 uur heeft de consument met haar bankpas en pincode een betaling gedaan van € 94,50 bij [naam kapper]. Op 24 juli 2020 heeft de consument met haar oma gewinkeld, waaronder bij [naam parfumerie]. Diezelfde dag heeft de consument bij [naam parfumerie] om 11:34 uur voor een betaling van € 4,48 gebruik gemaakt van contactloos betalen met haar bankpas.

2.3 Op 25 juli 2020 om 12:43 uur is met behulp van de bankpas en pincode van de consument een nieuw toestel gekoppeld aan de mobielbankieren applicatie van de consument. Diezelfde dag is er van de spaarrekening van de consument een bedrag van € 8.000,- overgemaakt naar de betaalrekening. Om 15:17 uur is met de bankpas van de consument een betaling gedaan bij het restaurant waar zij werkzaam is. Om 16:25 uur is de opnamelimiet van de bankpas van de consument naar € 10.000,- verhoogd via de mobielbankieren applicatie. Vervolgens is tussen 20:49 uur en 21:37 uur bij enkele geldautomaten in Utrecht in vijf delen een bedrag van € 8.160,- van de betaalrekening opgenomen met de bankpas en pincode van de consument.

2.4 Op 26 juli 2020 is van de spaarrekening een bedrag van € 5.300,- overgemaakt naar de betaalrekening van de consument. Diezelfde dag is tussen 07:15 uur en 07:17 uur het bedrag van € 5.300,- in drie delen opgenomen met de bankpas en pincode van de consument bij een geldautomaat in Utrecht.

2.5 Op 29 juli 2020 is een bedrag van € 9.000,- overgemaakt naar de betaalrekening van de consument. Diezelfde dag is tussen 14:50 uur en 14:56 uur in twee delen een bedrag van € 8.990,- opgenomen met de bankpas en pincode van de consument bij een geldautomaat in Amsterdam. De benadeelde derde heeft op 30 juli 2020 bij de politie aangifte gedaan van ‘fraude met betaalproducten’.

2.6 Op enig moment heeft de bank de mobielbankieren applicatie van de consument geblokkeerd. Tussen 1 en 2 augustus 2020 heeft de consument geprobeerd toegang te krijgen tot haar mobielbankieren applicatie. Op 3 augustus 2020 heeft een telefoongesprek plaatsgevonden tussen partijen, waarin de bank de consument heeft geïnformeerd dat haar betaalrekening, bankpas en mobielbankieren applicatie zijn geblokkeerd wegens fraude. Op 4 augustus 2020 heeft de consument het kantoor van de bank bezocht waar zij te horen kreeg dat de bank haar per brief nader zou informeren.

2.7 Op 9 augustus 2020 heeft de consument bij de politie telefonisch aangifte gedaan van ‘fraude met betaalproducten’.

2.8 Op 16 september 2020 heeft de bank de consument per brief geïnformeerd dat zij haar gegevens voor de maximale duur van acht jaar heeft opgenomen in het Incidentenregister en het Extern Verwijzingsregister (EVR) wegens medewerking aan fraude. De bank heeft vervolgens aangifte tegen de consument gedaan. Op 12 oktober 2020 heeft de consument via haar rechtsbijstandsverlener een klacht ingediend bij de bank.

2.9 De verdere uitwisseling van standpunten door partijen in de interne klachtprocedure heeft niet geleid tot een oplossing van de klacht.

De vordering en de klacht

2.10 De consument vordert van de bank € 14.000,- vermeerderd met wettelijke rente vanaf 26 oktober 2020. Ook vordert de consument van de bank herstel van de bankrelatie, het intrekken van de aangifte door de bank en het (met terugwerkende kracht) verwijderen van de interne en externe registraties.

2.11 De consument stelt allereerst dat de bank ten onrechte haar persoonsgegevens heeft opgenomen in de interne en externe registers. De consument heeft geen fraude gepleegd. De consument kwam pas laat erachter dat haar bankpas niet meer in haar handtas zat, omdat zij niet veel gebruik maakt van haar bankpas. De consument krijgt namelijk altijd cash fooi van haar bijbaan en cash geld van schoonmaakwerk bij haar oma. Daarnaast eet de consument vaak bij haar oma of vriend. De consument wist heel lang niet wat er aan de hand was. De consument dacht eerst dat er sprake was van een storing van de mobiel bankieren applicatie, aangezien zij een nieuwe telefoon had en niet alle applicaties goed werkten. Daarnaast heeft de consument geen pushberichten van de bank ontvangen, omdat dit alleen voorkomt in de mobiele applicatie. Deze mobiele applicatie heeft de consument niet gebruikt in de tijd dat de fraudeurs toesloegen. De consument stelt verder geen motief te hebben om fraude te plegen. De consument en haar familie zijn niet arm of kansloos; zij hebben geen ‘kleine vergoeding’ nodig. Er stond bijna € 14.000,- op de spaarrekening van de consument, waarvoor zij haar hele leven had gespaard. De oma en de vader van de consument beschikken ook over genoeg geld. Bovendien is het niet logisch dat iemand met eigen geld fraude gaat plegen. De consument stelt dat de bankpas door een derde is ontvreemd. De bankpas moet op 24 juli 2020 bij [naam parfumerie] uit de handtas van de consument zijn gestolen. Daarvóór moet de fraudeur de pincode van de consument gefilmd hebben.
Ten tweede stelt de consument dat de bank haar schadeloos dient te stellen. De bank heeft haar zorgplicht tegenover de consument geschonden. De transacties pasten immers niet bij het betaalgedrag van de consument.

De bank heeft nagelaten tijdig de bankrekening van de consument te blokkeren. Daarnaast is de beveiliging van de bank ondermaats tegen deze vorm van fraude. Iedereen kan met een universeel apparaat, bankpas en pincode transacties uitvoeren op de bankrekening van die persoon. Er was geen sprake van grove nalatigheid aan de zijde van de consument, nu zij aan al haar verplichtingen uit de voorwaarden van de bank heeft voldaan. Tot slot lijdt niet alleen de consument onder de fraudebeschuldiging, maar ook haar vader en de rest van de familie. De moeder van de consument is kortgeleden overleden. Haar vader loopt hierdoor bij een psycholoog om het verlies te verwerken.

Het verweer

2.12 De bank heeft verweer gevoerd tegen de stellingen van de consument. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Waar gaat het om?

3.1 In de kern gaat het geschil tussen partijen over de vraag of de bank de persoonsgegevens van de consument mocht opnemen in de interne en externe registers en of de bank gehouden is om de consument schadeloos te stellen.

Externe registers

Mocht de bank de persoonsgegevens van de consument registreren in de externe registers?

3.2 De beoordeling van de registraties van de persoonsgegevens van de consument in de registers (het EVR en het Incidentenregister) en de duur ervan moet plaatsvinden aan de hand van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen van 23 oktober 2013 (hierna: 'het Protocol').

3.3 Omdat opname van persoonsgegevens in deze registers – en met name het EVR – voor de consument ernstige gevolgen kan hebben (bijvoorbeeld geen hypotheek meer kunnen krijgen), moeten zware eisen worden gesteld aan de grond(en) van de bank voor opname van de persoonsgegevens van de consument.[1] Artikel 5.2.1 aanhef en onder a en b van het Protocol bepaalt onder welke voorwaarden persoonsgegevens mogen worden opgenomen in het EVR. Het moet gaan om gedragingen van de betrokkene die een bedreiging vormden, vormen of kunnen vormen voor de (financiële) belangen van een financiële instelling, en ook voor de continuïteit en integriteit van de financiële sector.

[1] Hof Arnhem-Leeuwarden 26 januari 2016, ECLI:NL:GHARL:2016:494, overweging 4.3, te vinden op www.rechtspraak.nl en Kifid GC 2017-717 onder 4.2, te vinden op www.kifid.nl

3.4 Uit een uitspraak van de Hoge Raad volgt verder dat voor het registreren van persoonsgegevens in het EVR is vereist dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld aan fraude door de betrokkene.[2] Het moet gaan om zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring in de zin van artikel 350 van het Wetboek van Strafvordering kunnen dragen. Een strafrechtelijke veroordeling is niet vereist. Anderzijds is de enkele verdenking van betrokkenheid bij een strafbaar feit in de zin van een vermoeden van schuld, zoals dat kan blijken uit een aangifte, niet voldoende.[3]

3.5 Als maatstaf heeft dus te gelden of de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan. Bij bevestigende beantwoording van deze vraag dient bovendien te worden beoordeeld of op grond van een en ander opneming in het Incidentenregister en het EVR gerechtvaardigd was en voor welke duur (artikel 6 onder f van de AVG, en artikel 5.2.1 sub c van het Protocol).

Is er sprake van een zwaardere verdenking dan een redelijk vermoeden van schuld?

3.6 De commissie is met de bank van oordeel dat voldoende is komen vast te staan dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld aan fraude. De gedragingen van de consument komen namelijk in voldoende mate overeen met de wijze waarop een zogenaamde 'money mule' oftewel 'geldezel' opereert.[4] De commissie gaat daarbij uit van het volgende.

a) *Aannemelijk dat de consument als geldezel heeft gefungeerd*

3.7 Allereerst merkt de commissie op dat de omstandigheden van dit geval passen bij het (gedrags)patroon van iemand die als geldezel fungeert, te weten derden die bekend zijn met de pincode, verhoging van de opnamelimiet via de mobielbankieren applicatie, de koppeling van een nieuwe toestel aan de mobiele applicatie, het leeghalen van de bankrekening vóór de storting van de frauduleus verkregen gelden en pas aangifte doen nadat de bankrekening al is geblokkeerd.[5] Dat de consument niet zelf de geldopnames heeft gedaan past ook bij dat patroon, nu een geldezel de persoon is die de eigen bankpas, pincode en de bankrekening ter beschikking stelt aan de fraudeur.

---

[2] Zie Hoge Raad 29 mei 2009, ECLI:NL:HR:2009:BH4720, overweging 4.4., te vinden op www.rechtspraak.nl
[3] Kifid GC 2018-377 overwegingen 4.2 en 4.3, te vinden op www.kifid.nl
[4] Zie o.a. Gerechtshof Arnhem-Leeuwarden 9 november 2017, ECLI:NL:GHARL:2017:10752, overweging 5.12, te vinden op www.rechtspraak.nl
[5] Zie o.a. Kifid GC 2021-0213, overweging 3.7, te vinden op www.kifid.nl

b) De consument maakte dagelijks gebruik van haar bankpas

3.8 Ten tweede blijkt uit de bankafschriften dat de consument, anders dan zij stelt, dagelijks gebruik maakte van haar bankpas. Ondanks dit dagelijks gebruik, stelt de consument dat zij tussen 24 juli 2020 en 2 augustus 2020 niet heeft opgemerkt dat zij haar bankpas niet meer in haar bezit had. In deze periode is met behulp van de bankrekening, de bankpas en pincode van de consument fraude gepleegd. Dat de consument nauwelijks gebruik maakte van haar bankpas, omdat zij genoeg cash had en dit verder ook niet nodig had, acht de commissie in dit verband niet als een voldoende aannemelijke verklaring. Daarnaast is het opmerkelijk dat op 25 juli 2020 de bankpas is gebruikt in het restaurant waar de consument werkt.

c) Verklaring over verlies bankpas en pincode niet aannemelijk

3.9 Ten derde slaagt het standpunt van de consument ten aanzien van haar afgekeken pincode bij [naam parfumerie] naar het oordeel van de commissie niet. Vaststaat dat de consument bij [naam parfumerie] heeft betaald door middel van contactloos betalen. De stelling van de consument dat zij bij haar eerste betaalpoging bij [naam parfumerie] een pincode heeft ingevuld, is daarentegen op geen enkele wijze door de consument onderbouwd. Het bestaan van de eerste pinpoging is daardoor niet komen vast te staan.

3.10 Verder acht de commissie het in de gegeven omstandigheden meer aannemelijk dat de consument direct contactloos heeft betaald bij de betaling van € 4,48 bij [naam parfumerie]. Dit baseert de commissie op de geringe hoogte van het bedrag, het betaalgedrag van de consument (veelal contactloze betalingen) en de eerdere betaling mét pincode bij [naam kapper]. Evenmin acht de commissie het waarschijnlijk dat de fraudeur de bankpas uit de handtas van de consument heeft kunnen zakkenrollen, gelet op de Covid-19 maatregelen die destijds golden.[6]

3.11 Daarnaast is niet aannemelijk dat een fraudeur ruim een dag wacht om misbruik te maken van een gestolen bankpas en pincode. Een fraudeur neemt namelijk niet het risico dat de bankpas wellicht al geblokkeerd is door het tijdsverloop. Wel acht de commissie het aannemelijk dat een fraudeur wacht met het gebruik maken van de bankpas en pincode als er geen risico is dat de pas wordt geblokkeerd en de gelden waarover hij of zij wil beschikken op een later tijdstip op de betreffende rekening zullen binnenkomen. Dat is ook in dit geval gebeurd, aangezien volgens de consument de bankpas op 24 juli 2020 is gestolen, vervolgens eerst al het spaargeld van de rekening is opgenomen waarna op 29 juli 2020 het geld afkomstig van fraude op haar bankrekening is bijgeschreven.

[6] Zie https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/vraag-en-antwoord/persconferentie-coronavirus-nieuwe-regels-per-1-juli-2020-in-eenvoudige-taal

3.12 Gelet op al het voorgaande is de commissie van oordeel dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld van de consument aan bankpasfraude door te fungeren als geldezel.

De proportionaliteit van de EVR-registratie

3.13 De bank dient bij de registratie het proportionaliteitsbeginsel in acht te nemen. Dit is neergelegd in artikel 5.2.1 sub c van het Protocol. Dit houdt in dat het belang van de financiële sector bij registratie moet worden afgewogen tegen de nadelige gevolgen voor de consument. Ook mag de duur van de registratie niet disproportioneel zijn. Betrokkenen die verwijdering of verkorting van de duur van hun registratie wensen, moeten aanvoeren waarom zij disproportioneel worden geraakt in hun belangen en waarom hun belangen zwaarder wegen dan die van de bank.

3.14 De bank heeft gemotiveerd aangevoerd waarom haar belang, het belang van haar klanten en dat van de financiële sector beschermd moet worden tegen personen die betrokken zijn bij oplichting. Volgens de bank vormen de gedragingen van de consument een bedreiging voor de (financiële) belangen van de bank en voor de continuïteit en/of integriteit van de financiële sector. Opname van de persoonsgegevens van de consument in het register is bedoeld om nieuwe gevallen van oplichting te voorkomen.

3.15 Gelet op het misbruik dat met de bankrekening van de consument heeft kunnen plaatsvinden, volgt commissie het standpunt van de bank dat het belang van de bank bij het extern registreren van zijn persoonsgegevens zwaarder weegt dan het belang van de consument. De commissie heeft kennisgenomen van hetgeen de consument heeft verklaard omtrent haar verloren familieleden, waaronder haar moeder. Hoewel de commissie betreurt dat de consument en de rest van haar familie dit verlies is overkomen, kunnen deze omstandigheden niet worden meegenomen in de beoordeling of de registratie(duur) proportioneel is. De consument heeft in dit verband onvoldoende onderbouwd waarom haar belang dient te prevaleren boven het belang van de bank in het kader van de proportionaliteit van de externe registratie van haar persoonsgegevens.

Mocht de bank de persoonsgegevens van de consument opnemen in het Incidentenregister?

3.16 Het EVR is gekoppeld aan het Incidentenregister (artikel 5.1.1 van het Protocol). Dit brengt mee dat zolang registratie in het EVR terecht en proportioneel is, de gegevens ook in het Incidentenregister blijven staan. Gelet op het bovenstaande dient ook de registratie in het Incidentenregister te worden gehandhaafd.

Interne registers

Voorwaarden registratie in de Gebeurtenissenadministratie en het IVR

3.17 Wat betreft de beantwoording van de vraag of de bank tot registratie in het IVR (dat aan de Gebeurtenissenadministratie is gekoppeld) mocht overgaan wordt het volgende overwogen.

3.18 Deze registers vormen het interne waarschuwingssysteem van de bank en de groep financiële ondernemingen waarvan de bank deel uitmaakt. Opname van de persoonsgegevens van de consument in het IVR brengt mee dat die gegevens ook in de Gebeurtenissen-administratie zijn opgenomen. Dit heeft als gevolg dat de commissie de vordering van de consument tot verwijdering van zijn gegevens uit het IVR aldus begrijpt dat daaronder ook de verwijdering van de gegevens uit de Gebeurtenissenadministratie moet worden begrepen.

3.19 Hiervóór is vastgesteld dat de bank de persoonsgegevens van de consument in het EVR heeft mogen opnemen, omdat sprake is van een zwaardere verdenking dan een redelijk vermoeden van (betrokkenheid bij) fraude. Deze vaststelling is op grond van artikel 33 lid 2 sub b UAVG voldoende om de registratie in de onderhavige registers te handhaven.

Proportionaliteit van de interne registraties

3.20 Aangezien de commissie hiervoor al heeft vastgesteld dat de registraties met externe werking in het EVR en het Incidentenregister terecht en proportioneel zijn, zijn ook de registraties in het IVR en de Gebeurtenissenadministratie toegestaan. De commissie merkt daarbij wel op dat het op de weg van de bank had gelegen om de consument al in haar brief van 16 september 2020 te wijzen op de opname van haar persoonsgegevens in deze interne registers. Dit laat echter onverlet dat de commissie registratie van de persoonsgegevens van de consument voor de van acht jaren terecht en proportioneel acht.

Geen grond voor de bank om schadeloos te stellen

3.21 Tot slot dient de commissie te beoordelen of de consument recht heeft op schadeloos-stelling door de bank. De commissie ziet hiertoe geen aanleiding vanwege het volgende.

3.22 Uit de vaste lijn van de geschillencommissie volgt dat er geen algemene signaleringsplicht van banken wordt aangenomen.[7] In de rol van betaaldienstverlener, zoals in dit geval, kan de bank in principe geen verwijt worden gemaakt voor het uitvoeren van transacties zonder nadere monitoring.

[7] Zie onder andere Kifid GC 2020-617, overweging 4.6, te vinden op www.kifid.nl

Van de bank mag dit onderzoek pas worden verwacht, wanneer er bij de bank sprake was van 'daadwerkelijk gevaarsbewustzijn'.[8] Van dit daadwerkelijk gevaarsbewustzijn bij de bank is niet dan wel onvoldoende gebleken.

3.23 Verder geldt op grond van de artikelen 7:528 en 7:529 van het Burgerlijk Wetboek (BW) dat de bank een niet-toegestane transactie dient te vergoeden aan de betaler, tenzij van de zijde van de betaler sprake is van grove nalatigheid ten aanzien van de verplichtingen uit artikel 7:524 BW, frauduleus handelen of opzettelijk handelen. Uit de vaste lijn van de geschillencommissie ten aanzien van niet-toegestane transacties volgt het volgende. Alhoewel het aan de bank is om te bewijzen dat sprake is geweest van *grove nalatigheid*, wat zich juridisch onderscheidt van *nalatigheid*, ligt het op de weg van de betaler (hier: de consument) om ten minste enig inzicht te geven in de wijze(n) waarop haar bankpas en pincode in onbevoegde handen zouden kunnen zijn geraakt.[9]

3.24 Naar het oordeel van de commissie heeft de consument onvoldoende inzicht gegeven in de wijze(n) waarop haar bankpas en pincode in onbevoegde handen zijn geraakt. De verklaringen die de consument heeft gegeven zijn naar het oordeel van de commissie onvoldoende aannemelijk om enige inzicht hierin te geven.

Conclusie

3.25 Gelet op het voorgaande is de commissie van oordeel dat de vordering van de consument dient te worden afgewezen.

4. De beslissing

De commissie wijst de vordering af.

Deze uitspraak is een bindend advies. Tegen deze uitspraak kunt u beroep instellen bij de Commissie van Beroep Financiële Dienstverlening als wordt voldaan aan de vereisten van artikel 2 van het Reglement van de Commissie van Beroep Financiële Dienstverlening. Voor het instellen van beroep geldt een termijn van zes weken na verzending van deze uitspraak. Het reglement van de commissie van beroep en meer informatie over het instellen van beroep kunt u vinden op de website www.kifid.nl/in-beroep-gaan-bij-kifid.

[8] Zie Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399, overweging 4.6, te vinden op www.rechtspraak.nl
[9] Zie onder andere Kifid GC nrs. 2011-7 (overweging 4.4), 2014-144 (overweging 4.8) en 2020-255 (overweging 4.6) te vinden op www.kifid.nl.

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.

Bijlagen

Relevante bepalingen uit wet- en regelgeving

Burgerlijk Wetboek Boek 7

Artikel 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 persoonlijke beveiligingsgegevens ervan te waarborgen.
3. De voorwaarden bedoeld in het eerste lid, onderdeel a, zijn objectief, niet-discriminerend en evenredig.

Artikel 527

1. Indien een betaaldienstgebruiker ontkent dat hij met een uitgevoerde betalingstransactie heeft ingestemd of aanvoert dat de betalingstransactie niet correct is uitgevoerd, is zijn betaaldienstverlener gehouden het bewijs te leveren dat de betalingstransactie is geauthenticeerd, juist is geregistreerd en geboekt en niet door een technische storing of enig ander falen van de door de betaaldienstverlener aangeboden diensten is beïnvloed. Indien de betalingstransactie geïnitieerd wordt via een betaalinitiatiedienstverlener, levert deze het bewijs dat, binnen zijn verantwoordelijkheid, de betalingstransactie is geauthenticeerd, juist is geregistreerd en niet door een technische storing of enig ander falen in verband met de betaaldienst waarmee hij is belast, is beïnvloed.
2. Indien een betaaldienstgebruiker ontkent dat hij met een uitgevoerde betalingstransactie heeft ingestemd, vormt het feit dat het gebruik van een betaalinstrument door de betaaldienstverlener, daaronder in voorkomende geval de betaalinitiatiedienstverlener begrepen, is geregistreerd niet noodzakelijkerwijze afdoende bewijs dat met de betalingstransactie door de betaler is ingestemd of dat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer van zijn verplichtingen uit hoofde van artikel 524 niet is nagekomen. De betaaldienstverlener, daaronder in voorkomend geval de betaalinitiatiedienstverlener begrepen, verstrekt ondersteunend bewijs om fraude of grove nalatigheid van de zijde van de betaler te bewijzen.

Artikel 528

1. Onverminderd artikel 526, betaalt de betaaldienstverlener van de betaler, in geval van een niet-toegestane betalingstransactie, de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransactie terug en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, nadat hij bekend is geworden met de transactie of daarvan in kennis is gesteld.

2. Op grond van het eerste lid herstelt de betaaldienstverlener van de betaler de betaalrekening die met dat bedrag is gedebiteerd in de toestand zoals die geweest zou zijn wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden. De valutadatum van de creditering van de betaalrekening van de betaler is uiterlijk de datum waarop het bedrag was gedebiteerd.

3. Het eerste lid is niet van toepassing indien de betaaldienstverlener van de betaler redelijke gronden heeft om fraude te vermoeden en hij deze gronden schriftelijk aan de Autoriteit Financiële Markten meedeelt.

4. Indien de betalingstransactie via een betaalinitiatiedienstverlener wordt geïnitieerd, betaalt de rekeninghoudende betaaldienstverlener onmiddellijk, en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, 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 wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden.

5. Ingeval de betaalinitiatiedienstverlener aansprakelijk is voor de niet-toegestane betalingstransactie, vergoedt hij de rekeninghoudende betaaldienstverlener op diens verzoek onmiddellijk de geleden verliezen of de aan de betaler terugbetaalde bedragen, waaronder het bedrag van de niet-toegestane betalingstransactie. Overeenkomstig artikel 527, tweede lid, is de betaalinitiatiedienstverlener gehouden te bewijzen dat, binnen zijn verantwoordelijkheid, de betalingstransactie is geauthenticeerd, juist is geregistreerd en niet door een technische storing of enig ander falen in verband met de betaaldienst waarmee hij is belast, is beïnvloed.

6. Aanvullende financiële compensatie kan worden vastgesteld overeenkomstig het recht dat van toepassing is op de tussen de betaler en zijn betaaldienstverlener gesloten overeenkomst of de tussen de betaler en de betaalinitiatiedienstverlener gesloten overeenkomst, indien van toepassing.

Artikel 529

1. 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.

2. 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 lid van dit artikel bedoelde aansprakelijkheid beperken, met name rekening houdend met de aard van de persoonlijke beveiligingsgegevens van het betaalinstrument en met de omstandigheden waarin het is verloren, gestolen of onrechtmatig gebruikt.

3. Indien de betaaldienstverlener van de betaler geen sterke cliëntauthenticatie verlangt, draagt de betaler geen financiële verliezen, tenzij de betaler frauduleus heeft gehandeld. Indien de sterke cliëntauthenticatie door de begunstigde of de betaaldienstverlener van de begunstigde niet wordt aanvaard, wordt de door de betaaldienstverlener van de betaler geleden financiële schade door hen vergoed.
4. Na de kennisgeving overeenkomstig artikel 524, eerste lid, onder b, heeft het gebruik van het betaalinstrument geen financiële gevolgen voor de betaler, tenzij deze frauduleus heeft gehandeld.
5. Indien de betaaldienstverlener nalaat om overeenkomstig artikel 525, eerste lid, onder c, passende middelen beschikbaar te stellen waarmee te allen tijde een kennisgeving als bedoeld in artikel 524, eerste lid, onder b, kan worden gedaan, is de betaler niet aansprakelijk voor de financiële gevolgen die uit het gebruik van dat betaalinstrument voortvloeien, tenzij hij frauduleus heeft gehandeld.

Relevante artikelen uit het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen van 23 oktober 2013

In het toepasselijke Protocol Incidentenwaarschuwingssysteem Financiële Instellingen van 23 oktober 2013 zijn de volgende relevante bepalingen opgenomen:

2. Begripsbepalingen

In dit protocol wordt verstaan onder:
Incident: een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van de cliënten of medewerkers van een Financiële Instelling, de Financiële Instelling zelf of de financiële sector als geheel in het geding zijn of kunnen zijn, zoals het falsificeren van nota's, identiteitsfraude, skimming, verduistering in dienstbetrekking, phishing en opzettelijke misleiding.

3.1 Incidentenregister en Extern Verwijzingsregister
3.1.1 Iedere Deelnemer heeft een Incidentenregister, waarin door de betreffende Deelnemer gegevens van (rechts)personen worden vastgelegd ten behoeve van het in artikel 4.1.1 Protocol genoemde doel, naar aanleiding van of betrekking hebbend op een (mogelijk) Incident. (…)
3.1.2 Aan het Incidentenregister is een Extern Verwijzingsregister gekoppeld. (…)

4 Incidentenregister

4.1 Doel Incidentenregister
4.1.1 Met het oog op het kunnen deelnemen aan het Waarschuwingssysteem is iedere Deelnemer gehouden de volgende doelstelling voor het vastleggen van gegevens in het Incidentenregister te hanteren:
"Het geheel aan verwerkingen ten aanzien van het Incidentenregister heeft tot doel het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de financiële sector, daaronder mede begrepen (het geheel van) activiteiten die gericht zijn:
- op het onderkennen, voorkomen, onderzoeken en bestrijden van gedragingen die kunnen leiden tot benadeling van de branche waar de financiële instelling deel van uitmaakt, van de economische eenheid (groep) waartoe de financiële instelling behoort, van de financiële instelling zelf, alsmede van haar cliënten en medewerkers;
- op het onderkennen, voorkomen, onderzoeken en bestrijden van oneigenlijk gebruik van producten, diensten en voorzieningen en/of (pogingen) tot strafbare of laakbare gedragingen en/of overtreding van (wettelijke) voorschriften, gericht tegen de branche waar de financiële instelling deel van uitmaakt, de economische eenheid (groep) waartoe de financiële instelling behoort, de financiële instelling zelf, alsmede haar cliënten en medewerkers;
- op het gebruik van en de deelname aan waarschuwingssystemen."

4.2 Toegang tot het Incidentenregister
(…)
4.2.3 De gegevens uit het Incidentenregister van de Deelnemer mogen tevens worden uitgewisseld met functionarissen werkzaam bij de daartoe ingerichte, coördinatiefuncties van de NVB, Verbond, VFN, ZN, FOV en SFH (de fraudeloketten).
(…)
4.3 Verwijdering van gegevens uit het Incidentenregister
(…)

4.3.2 Verwijdering van gegevens uit het Incidentenregister moet plaatsvinden uiterlijk 8 jaar na opname van het betreffende gegeven in het Incidentenregister, tenzij zich ten aanzien van de betreffende (rechts)persoon een nieuwe aanleiding heeft voorgedaan die opnamen in het Incidentenregister rechtvaardigt.

5 Extern Verwijzingsregister

5.1 Functie van het Extern Verwijzingsregister

5.1.1 Volledige en ongecontroleerde toegang tot het Incidentenregister van een Deelnemer door de overige Deelnemers is niet wenselijk. Daarom is er voor gekozen aan het Incidentenregister een Extern Verwijzingsregister te koppelen. In het Extern Verwijzingsregister zijn uitsluitend Verwijzingsgegevens opgenomen. Het Extern Verwijzingsregister is raadpleegbaar door de (Organisaties van de) Deelnemers. Nadat door een Deelnemer wordt vastgesteld dat een (rechts)persoon is opgenomen in het Externe Verwijzingsregister, zijn volgens het bepaalde in artikel 4.2 Protocol gegevens uit het Incidentenregister voor de Deelnemer beschikbaar. Op deze wijze worden gegevens uit het Incidentenregister op een zorgvuldige en gecontroleerde wijze beschikbaar voor de (Organisaties van de) Deelnemers.

5.2 Vastlegging van gegevens in het Extern Verwijzingsregister

5.2.1 De Deelnemer dient de Verwijzingsgegevens van (rechts)personen die aan de hierna onder a en b vermelde criteria voldoen en na toepassing van het onder c genoemde proportionaliteitsbeginsel op te nemen in het Extern Verwijzingsregister.

a) De gedraging(en) van de (rechts)persoon vormden, vormen of kunnen een bedreiging vormen voor (I) de (financiële) belangen van cliënten en/of medewerkers van een Financiële instelling, alsmede de (Organisatie van de) Financiële instelling(en) zelf of (II) de continuïteit en/of de integriteit van de financiële sector.

b) In voldoende mate staat vast dat de betreffende (rechts)persoon betrokken is bij de onder a bedoelde gedraging(en). Deze vaststelling betekent dat van strafbare feiten in principe aangifte of klachten wordt gedaan bij een opsporingsambtenaar.

c) Het proportionaliteitsbeginsel wordt in acht genomen. Dit houdt in dat Veiligheidszaken vaststelt, dat het belang van opname in het Externe Verwijzingsregister prevaleert boven de mogelijk nadelige gevolgen voor de Betrokkene als gevolg van opname van zijn Persoonsgegevens in het Extern Verwijzingsregister.

5.3 Verwijdering van gegevens uit het Extern Verwijzingsregister

(…)

5.3.2 Verwijdering van Verwijzingsgegevens uit het Extern Verwijzingsregister moet plaatsvinden uiterlijk 8 jaar na opname van het betreffende gegeven in het Incidentenregister, tenzij zich ten aanzien van de betreffende (rechts)persoon een nieuwe aanleiding heeft voorgedaan en opname in het Extern Verwijzingsregister conform artikel 5.2.1 Protocol heeft plaatsgevonden.

Relevante artikelen uit de AVG

Artikel 6
Rechtmatigheid van de verwerking
1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
(…)
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Artikel 10
Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.

Relevante artikelen uit de UAVG

Artikel 33. Overige uitzonderingsgronden inzake gegevens van strafrechtelijke aard
(…)
2 *Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt:*
(…)
b. *ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.*
(…)
4 *Persoonsgegevens van strafrechtelijke aard mogen ten behoeve van derden worden verwerkt:*
(…)
b. *indien deze derde een rechtspersoon is die in dezelfde groep is verbonden als bedoeld in artikel 24b van Boek 2 van het Burgerlijk Wetboek (…)*