

# Indsigelse mod transaktioner i forbindelse med telefonisk henvendelse. Spørgsmål om groft uforsvarlig adfærd.

Sagsnummer: 356/2018

Dato: 07-11-2019

Ankenævn: Vibeke Rønne, Inge Kramer, Peter Stig Hansen, Morten Bruun Pedersen, Poul Erik Jensen.

Klageemne: Netbank - øvrige spørgsmål  
Betalings tjenester - ikke-vedkendte hævnings  
Betalings tjenester - ikke groft uforsvarlig adfærd

Ledetekst: Indsigelse mod transaktioner i forbindelse med telefonisk henvendelse. Spørgsmål om groft uforsvarlig adfærd.

Indklagede: Danske Andelskassers Bank

Øvrige  
oplysninger:

Senere dom:

*Pengeinstitutter*

---

Klager medhold.

## Indledning

Denne sag vedrører indsigelse mod transaktioner i forbindelse med telefonisk henvendelse.

## Sagens omstændigheder

Klageren er kunde i Danske Andelskassers Bank, hvor hun har en konto med et tilknyttet VISA-Dankort samt adgang til netbank. Banken har oplyst, at klageren den 21. februar 2018 fik tilknyttet såkaldt 3D Secure til sit mobilnummer.

Den 10. august 2018 kl. 18.16.29 blev der med klagerens VISA-Dankort foretaget en transaktion på 7.989,00 kr. på klagerens konto. Kl. 18.43.13 samme dag blev der foretaget en yderligere transaktion på 8.559,17 kr., i alt 16.548,17 kr. Beløbene blev hævet på klagerens konto med valør den 14. august 2018.

Banken har anført, at betalingsmodtagerne antages at være pengeoverførselsvirksomheder, og at det formodes, at beløbene er videreoverført til konti i udlandet.

Den 16. august 2018 underskrev klageren en indsigelsesblanket med tro- og loveerklæring, hvor hun gjorde indsigelse mod de to transaktioner på i alt 16.548,17 kr., samt en eventuel yderligere transaktion på 8.011,04 kr. Klageren anførte, at hun hverken havde deltaget i eller godkendt transaktionerne, at kortet var i hendes besiddelse på tidspunktet for de ikke-godkendte transaktioner, og at kortet var blevet spærret den 10. august 2018. Klageren anførte endvidere blandt andet:

"...

Jeg bliver den 10.08.2018 ringet op af dem, der giver sig ud for at være Microsoft. De siger, at jeg er blevet hacket på min computer og at de vil hjælpe mig hermed.

De beder mig oplyse mit kortnummer og det giver jeg dem.

De er også inde på min netbank, mens jeg kigger med.

Samme aften (imens samtalen er i gang) modtager jeg sms'er fra Nets, der beder mig bekræfte, at jeg er i gang med at foretage korttransaktionerne, som jeg nu gør indsigelse imod.

Jeg bekræfter IKKE disse transaktioner.

..."

Den eventuelle transaktion på 8.011,04 kr., der var nævnt i indsigelsen, blev ikke gennemført.

Den 10. oktober 2018 godtgjorde banken klageren 8.548,17 kr. af de i alt 16.548,17 kr., idet det var bankens opfattelse, at klageren som følge af groft uforsvarlig adfærd hæftede for 8.000 kr., jf. betalingsloven § 100, stk. 4, nr. 3.

I en e-mail af 12. oktober 2018 til banken anførte klageren blandt andet:

"...

Microsoft siger, at jeg skal fornye en licence, hvilket jeg gør med mit kontokort. Den sum er 199,- og bliver aldrig hævet. ...

De beder mig om at åbne min konto for at se om der er trojanske heste der.

... De bad mig aldrig om at installere noget på mobilen. Jeg kan heller ikke forklare hvordan nogen, sandsynligvis dem, kan bruge mit mobilnummer til at ringe til Polen med, hvilket de gør et par timer senere samme dag (det kan jeg se på min telefonregning jeg modtog fra [telefonselskab] for nogle dage siden) mens min mobil ligger trygt i min inderlomme hele resten af aftenen

...Jeg stolede på at jeg modtog hjælp og jeg blokerede straks min konto da jeg havde mulighed for at læse mine sms fra NETS. Sagen er meldt til politiet og de mener ikke, at jeg har handlet groft uforsvarlig. ...

..."

Ved et brev af 31. oktober 2018 til klageren fastholdt banken, at klageren hæftede for 8.000 kr., jf. betalingsloven § 100, stk. 4, nr. 3.

Den 7. november 2018 indgav klageren en klage over banken til Ankenævnet.

Ved en e-mail af 21. november 2018 spurgte banken Nets, om de to transaktioner på i alt 16.548,17 kr. var godkendt med sms-kode eller med nemid. Ved en e-mail af 7. december 2018 til banken oplyste Nets, at transaktionerne var valideret med nemid. Nets sendte diverse udskrifter, herunder logbog og autorisationsforespørgsler samt en udskrift, der viste, at der den 10. august 2018 var blevet sendt tre 3D Secure koder til klagerens telefonnummer henholdsvis kl. 18.14.37, kl. 18.41.25 og kl. 18.55.52. Ifølge den fremlagte log blev tre nøglekoder fra klagerens fysiske nemid nøglekort accepteret den 10. august 2018 henholdsvis kl. 18.16.20, kl. 18.43.08 og kl. 18.58.14.

Af bankens "Vilkår for Netbank" fremgår blandt andet:

"...

#### **4. Kundens ansvar**

4.1 Bestemmelserne i dette pkt. 4 finder kun anvendelse, når kunden benytter Netbanks betalingstjenester. ...

4.2 I tilfælde af, at kundens Netbank-adgang har været misbrugt af en anden person, vil Danske Andelskassers Bank A/S dække tabet, medmindre tabet er omfattet af en af bestemmelserne nedenfor.

4.3 Kunden skal dække tab op til kr. 375 (selvrisiko), hvis Netbank-adgangen er misbrugt af en anden ved anvendelse af kundens personlige sikkerhedsoplysninger.

4.4 Kunden skal dække tab op til kr. 8.000 i tilfælde af, at kundens personlige sikkerhedsoplysninger har været anvendt, og

a) ... eller

b) kunden har oplyst sine personlige sikkerhedsoplysninger til den, der har foretaget den uberettigede anvendelse, uden at kunden indså eller burde have indset, at der var risiko for misbrug, eller

c) kunden ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

4.5 ...

...

4.8 Kunden er kun ansvarlig i henhold til pkt. 4.3, 4.4 og 4.5, såfremt transaktionerne er korrekt registreret og bogført.

..."

Af bankens "Brugerregler – Visa/Dankort" fremgår blandt andet:

"...

## **6 Sikre internetbetalinger**

"Verified by Visa" og "Dankort Secured by Nets" er en ekstra beskyttelse mod misbrug af kortdata ved handel på internettet.

Sikkerheden består i, at du ved køb på internettet efter indtastning af kortoplysninger skal benytte en engangskode, som du modtager fra Nets via SMS i forbindelse med betalingen. Engangskoden skal kun anvendes ved køb i internetforretninger, der anvender denne ekstra beskyttelse.

### **6.1 Tilmelding**

Inden eller senest i forbindelse med dit første køb i en forretning, der anvender "Dankort Secured by Nets" eller "Verified by Visa", skal du tilmelde dit kort.

Hvis du har tilmeldt dit Visa/Dankort til "Verified by Visa", vil dette også gælde som tilmelding til "Dankort Secured by Nets" og omvendt.

Tilmelding kan enten ske via Danske Andelskassers Bank A/Ss hjemmeside eller netbank eller i forbindelse med dit første køb. I forbindelse med tilmelding skal du også angive det mobiltelefonnummer, som du vil bruge til at modtage engangskoder på. ...

...

### **6.2 Sikkerhed - kort og telefon**

Da din mobiltelefon bliver en del af sikkerheden ved internetkøb i forretninger, der benytter "Dankort Secured by Nets" eller "Verified by Visa", skal du sikre, at andre ikke har eller kan få uhindret adgang til både dit kort og din mobiltelefon. Vi anbefaler derfor, at du anvender en kode til din mobiltelefon.

...

## **11 dit ansvar ved misbrug af dit Visa/Dankort**

### **11.1 Dækning af tab**

I tilfælde af, at dit Visa/Dankort har været misbrugt af en anden person vil Danske Andelskassers Bank A/S dække tabet, medmindre tabet er omfattet af afsnit 11.2 og 11.3 nedenfor. Det er Danske Andelskassers Bank A/S, der skal bevise, at tabet er omfattet af afsnit 11.2 og 11.3.

### 11.2 Hæftelse og selvrisko

Hvis dit Visa/Dankort er blevet misbrugt af en anden person og der i den forbindelse er anvendt pinkode, skal du dække op til 375 kr. af det samlede tab.

...

Du skal dække tab op til 8.000 kr. i tilfælde af, at dit Visa/Dankort har været misbrugt af en anden person og der i den forbindelse er anvendt pinkode, og

\* ...

\* du med forsæt har overgivet pinkoden til den, der har foretaget den uberettigede anvendelse, uden at du indså eller burde have indset, at der var risiko for misbrug

\* du ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

..."

### Parternes påstande

Den 7. november 2018 har klageren indbragt sagen for Ankenævnet med påstand om, at Danske Andelskassers Bank skal betale 8.000 kr.

Danske Andelskassers Bank har nedlagt påstand om principalt frifindelse, subsidiært afvisning.

### Parternes argumenter

**Klageren** har anført, at transaktionerne ikke er sket med hendes samtykke. Hun har på ingen måde godkendt transaktionerne, herunder hverken med nemid eller sms-koder.

Hun blev den 10. august 2018 ringet op af firmaet Microsoft, som fortalte, at hun havde problemer med sin computer, blandt andet trojanske heste, og at de meget gerne vil hjælpe hende. Personen, der ringede, præsenterede sig med navn og ansættelsesnummer.

Først skulle hun forny licensen, hvilket hun betalte med kontokort. Derefter blev hun bedt om at installere et program på sin computer, så de kunne hjælpe hende, hvilket hun gjorde.

De bad hende gå ind på netbank, så de kunne se om der var trojanske heste der. Personen fandt ikke noget og samtalen blev afsluttet.

Hun opbevarede sit nøglekort i hjemmet. Hun havde ingen kopier af kortet hverken på mobil eller computer. Hun havde sit nemid-nøglekort fremme og brugte det til at logge ind på netbanken. Derefter lagde hun det væk. Hun oplyste ikke nøgler fra kortet til andre.

Efter samtalen opdagede hun, at hun havde modtaget sms-koder fra Nets. Hun anvendte ikke sms-koderne men blokerede i stedet straks sin konto. Transaktionerne blev gennemført alligevel.

Hendes telefonnummer blev hacket og misbrugt til en udenlandssamtale om aftenen den 10. august 2018.

Hun har anmeldt sagen til politiet.

Banken bør anerkende, at hun er blevet udsat for svindel og er blevet groft snydt af professionelle bedragere, og at ikke at hun ikke har handlet groft uforsvarligt.

Politiet anerkender det som bedrag og en moderne form for tricktyveri. Hendes telefonselskab anerkender det også, da hun ikke skal betale for udlandssamtalen.

**Danske Andelskassers Bank** har til støtte for frifindelsespåstanden anført, at klageren bør hæfte for 8.000 kr. i medfør af betalingsloven § 100, stk. 4, nr. 3.

De omhandlede transaktioner blev foretaget og verificeret med indtastning af nemid nøglekode fra klagerens fysiske nøglekort og sms-koder til klagerens telefonnummer. Tidspunkterne for anvendelse af nøglekoder og sms-koder var overensstemmende med transaktionstidspunkterne.

Klageren har handlet groft uforsvarligt og derved muliggjort den uberettigede anvendelse af hendes VisaDankort, ved at have oplyst både sit kontonummer og sit VisaDankort nummer samt installere et program på sin computer og efterfølgende logge på sin netbank for at lade en fremmed person få adgang til hendes private netbank via en fjernopkobling gennem det installerede program. Klageren burde have indset, at der var risiko for misbrug af hendes VisaDankort og hendes netbank.

Banken har ikke registreret tekniske fejl eller svigt, og det kan efter bankens vurdering lægges til grund, at transaktionerne er korrekt registreret og bogført.

Banken har til støtte for afvisningspåstanden anført, at idet beløbene er overført til betalingsformidler må banken antage, at det er i overensstemmelse med klager, idet klager har udleveret de oplysninger, der skulle til, for at transaktionerne kunne foretages.

Klageren har valideret overførslerne med nemid, hvorfor betalingerne skal anses for gennemført ved hjælp af personlig sikkerhedsforanstaltning.

Det forudsætter bevisførelse ved partsforklaring at afklare nærmere, hvorvidt transaktionerne er sket med klagers samtykke, eller hvorvidt transaktionerne er uautoriserede.

#### **Ankenævnets bemærkninger**

Klageren har gjort indsigelse mod to transaktioner på henholdsvis 7.989,00 kr. og 8.559,17 kr., som den 10. august 2018 henholdsvis kl. 18.16.29 og kl. 18.43.13 blev foretaget med klagerens VISA-Dankort, der var udstedt af Danske Andelskassers Bank. De i alt 16.548,17 kr. blev hævet på klagerens konto i banken med valør den 14. august 2018.

Ifølge oplysninger fra Nets blev transaktionerne valideret med klagerens Nemid.

Baggrunden for transaktionerne var, at klageren den samme dag blev kontaktet telefonisk af en mand, M, der udgav sig for at være fra Microsoft. M oplyste, at klagerens computer var hacket, og tilbød at hjælpe klageren. Klageren har oplyst, at hun efter anmodning fra den pågældende oplyste sit kortnummer og betalte fornyet licens på 199 kr., men at denne transaktion aldrig blev gennemført. Klageren efterkom endvidere en anmodning fra M om at installere et program på sin computer, og klageren loggede på sin netbank med Nemid. Klageren havde et fysisk Nemid-nøglekort. Klageren har oplyst, at hun havde nøglekortet fremme og brugte det til at logge ind på netbanken. Derefter lagde hun det væk. Hun oplyste ikke nøgler fra kortet til andre.

Klageren konstaterede efterfølgende, at der var blevet sendt tre 3D Secure koder til hendes mobiltelefon henholdsvis kl. 18.14.37, kl. 18.41.25 og kl. 18.55.52. Klageren har oplyst, at hun ikke anvendte koderne, men i stedet spærrede sin konto.

Ankenævnet finder, at transaktionerne skyldtes tredjemands misbrug af klagerens Nemid. Det lægges endvidere til grund, at transaktionerne er korrekt registreret og bogført og ikke er ramt af tekniske svigt eller andre fejl, jf. betalingslovens § 98, stk. 1. Efter bestemmelsens stk. 2 er registrering af brug af et betalingsinstrument ikke i sig selv bevis for, at betaleren har godkendt transaktionen, at betaleren har handlet svigagtigt, eller at betaleren har undladt at opfylde sine forpligtelser, jf. betalingslovens § 93.

Ankenævnet finder, at klagerens Nemid er en personlig sikkerhedsforanstaltning, jf. betalingsloven § 7, nr. 31. Ved transaktionen blev der anvendt stærk kundeautentifikation, jf. betalingsloven § 7, nr. 30.

Efter betalingslovens § 100, stk. 5, hæfter betaleren uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, og betalerens udbyder godtgør, at betaleren med forsæt har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug. Ankenævnet finder ikke, at banken har godtgjort, at betingelserne for, at klageren hæfter uden beløbsbegrænsning efter betalingslovens § 100, stk. 5 er opfyldt.

Efter betalingslovens § 100, stk. 4, nr. 2 og 3 hæfter betaleren med op til 8.000 kr. af tabet som følge af andres uberettigede anvendelse, hvis betalerens udbyder godtgør, at betaleren med forsæt har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 5, eller at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

Tre medlemmer – Vibeke Rønne, Morten Bruun Pedersen og Poul Erik Jensen – udtaler:

Vi lægger til grund, at klageren er blevet franarret sin personlige sikkerhedsforanstaltning. På denne baggrund og efter det i øvrigt fremkomne finder vi ikke, at banken har godtgjort, at betingelserne for, at klageren hæfter efter de udvidede ansvarsbestemmelser i betalingslovens § 100, stk. 4 eller 5, er opfyldt. Klagerens hæftelse for tabet på 16.548,17 kr. udgør herefter højst 375 kr., jf. betalingslovens § 100, stk. 3.

Banken har før klageren klagede til Ankenævnet godtgjort klageren 8.548,17 kr. af de i alt 16.548,17 kr.

Vi stemmer derfor for, at banken skal godtgøre klageren yderligere 7.675 kr. ved at indsætte dette beløb på klagerens konto med valør den 14. august 2018.

To medlemmer – Inge Kramer og Peter Stig Hansen – udtaler:

Vi finder, at klageren ved groft uforsvarlig adfærd har muliggjort transaktionen, og at klageren som følge heraf hæfter med op til 8.000 kr.

Vi stemmer derfor for, at klageren ikke får medhold i klagen.

Der træffes afgørelse efter stemmeflertallet.

### **Ankenævnets afgørelse**

Danske Andelskassers Bank skal inden 30 dage indsætte 7.625 kr. på klagerens konto med valør den 14. august 2018.