

## Indsigelse mod netbank-transaktioner i forbindelse med telefonisk henvendelse fra en person, der udgav sig fra at være fra Nets. Videregivelse af NemID-oplysninger og SMS-koder.

Sagsnummer: 285/2020

Dato: 05-03-2021

Ankenævn: Henrik Waaben, Inge Kramer, Kristian Ingemann Petersen, Morten Bruun Pedersen, Anna Marie Schou Ringive.

Klageemne: Betalingstjenester - groft uforsvarlig adfærd  
Betalingstjenester - ikke groft uforsvarlig adfærd  
Betalingstjenester - ubegrænset hæftelse  
Netbank - øvrige spørgsmål

Ledetekst: Indsigelse mod netbank-transaktioner i forbindelse med telefonisk henvendelse fra en person, der udgav sig fra at være fra Nets. Videregivelse af NemID-oplysninger og SMS-koder.

Indklagede: Middelfart Sparekasse

Øvrige oplysninger: IF

Senere dom:  
*Pengeinstitutter*

---

Klager medhold.

### Indledning

Sagen vedrører indsigelse mod netbank-transaktioner i forbindelse med telefonisk henvendelse fra en person, der udgav sig fra at være fra Nets. Videregivelse af Nem ID-oplysninger og SMS-koder.

### Sagens omstændigheder

Klageren var kunde i Middelfart Sparekasse, hvor hun blandt andet havde en lønkonto -420, en konto -353 samt netbankadgang.

Den 20. juni 2019 blev klageren kontaktet af en mand, M, som udgav sig for at være fra Nets. M fortalte, at der var nogen, som var i færd med at hacke klagerens konto, hvilket M kunne afværge, hvis klageren videregav nogle oplysninger.

Herefter udleverede klageren i første omgang CPR-nummer og personlig kode og efterfølgende NemID-nøglekode, således, at M fik mulighed for at logge ind på klagerens netbank.

Efterfølgende modtog klageren over et tidsrum på ca. 30 minutter (fra kl. 14:04 til 14:33) seks SMS'er, som M fortalte klageren, at M skulle bruge for at standse hackerangrebet. Anvendelsen af SMS-engangskoder var en ekstra sikkerhed, når overførslerne var over en vis størrelse. Sparekassen har oplyst, at SMS'erne havde følgende ordlyd:

"Denne kode må aldrig udleveres til andre. Indtast engangskode: xxxxxx i Netbank, for at godkende betalingen. Er du ikke i gang med en betaling, kontakt straks dit pengeinstitut og/eller få spærret dit NemID".

Klageren videregav SMS-koderne til M.

Der blev herefter iværksat seks overførsler fra klagerens konti: en overførsel på 13.000 kr. og fire overførsler på 15.000 kr. fra konto -420 og en overførsel på 250.000 kr. fra konto -353, i alt 323.000 kr.

Dagen efter hændelsen, den 21. juni 2019, omkring kl. 10, kontaktede klageren sparekassen, der igangsatte forebyggende foranstaltninger.

Den 21. juni 2019 indgav klageren ligeledes en politianmeldelse.

Ved en tro- og loveerklæring af 24. juni 2020 gjorde klageren indsigelse over for sparekassen mod uretmæssige hævnninger på i alt 323.000 kr. Af rubrikken "Detaljeret beskrivelse af hændelsesforløbet" fremgik følgende:

"Min kæreste [navn], modtager opkald 13.58, 20/6-2019, hvor en [navn] ønsker at tale med mig. Jeg taler med ham og han fortæller at mine bankkonti er ved at blive hacket, hvorfor jeg skal hjælpe ham med at afværge dette. Jeg spørger ham hvem her og hvor han ringer fra, og, han fortæller at han er fra nets, og jeg kan slå ham op på nettet – det gør jeg, og finder ham også. Han taler mig hen i at skulle have div. oplysninger, herunder nemid og sms koder, for at kunne hjælpe mig med at beskytte mine konti. Forløbet på tlf er ca. 60 min. varighed, og afsluttes med at jeg bliver informeret om at min tlf skal være slukket i 2 timer, inden den må genstartes."

I en efterfølgende mail af 27. juni 2019, hvori klageren besvarede nogle uddybende spørgsmål fra sparekassen om, hvornår hun fik mistanke om, hvad der var sket, og om hun kunne se telefonnummer i opkaldslisten på telefonen, svarede klageren:

"Du spørger om yderligere oplysninger i hændelsesforløbet.

Efter sådan et forløb er jeg nok lidt chokeret. Derfor rører jeg ikke min telefon mere den dag. Jeg er på festival, hvor jeg er frivillig hjælper, og fortæller nogle få andre hvad der er sket. Jeg tror det er der det går op for mig, at jeg er blevet hacket. Det telefonnr. der bliver ringet fra er [telefonnummer 1]. KL. 17.49 ringer det samme nr. 7 gange, men [navn] (min kæreste) besvarer ikke opkaldet. Der er også andre numre der ringer kl. 18.52 [telefonnummer 2] 2 gange, og [telefonnummer 3] 1 gang. ..."

Sparekassen har oplyst, at det lykkedes at få tilbageført 149.600 kr. til klageren, og at tabet herefter udgjorde 173.400 kr.

Sparekassen afviste at tilbageføre tabet på 173.400 kr. til klageren.

### **Parternes påstande**

Den 29. juli 2020 har klageren indbragt sagen for Ankenævnet med påstand om, at Middelfart Sparekasse skal tilbageføre 173.400 kr. med fradrag af enten 375 kr. eller 8.000 kr.

Middelfart Sparekasse har nedlagt påstand om principalt frifindelse, subsidiært afvisning.

### Parternes argumenter

**Klageren** har blandt andet anført, at sparekassen skal betale beløbet, medmindre sparekassen dokumenterer, at betalingslovens § 100, stk. 5, finder anvendelse. Sparekassen har således bevisbyrden for, at kravet er omfattet af betalingslovens § 100, stk. 5, og at kravet som følge heraf er bortfaldet.

Sparekassen skal i denne sammenhæng dokumentere, at hun med forsæt har oplyst sine personlige sikkerhedsforanstaltninger, og at hun på dette tidspunkt indså eller burde have indset, at der var risiko for misbrug. Efter Ankenævnets praksis er dette ikke tilfældet i nærværende sag, jf. eksempelvis Ankenævnets afgørelser (207/2019, 280/2019 og 373/2019) samt UfR 2019.B.339.

I Ankenævnets afgørelse 373/2019 blev der modtaget 15 SMS'er over en periode på 29 minutter, og hun modtog seks SMS'er over en periode på 29 minutter. Herudover er der en række andre lighedspunkter mellem de to sager, der medfører, at nærværende sag kan sidestilles med Ankenævnets afgørelse 373/2019, således at hun har krav på betaling fra Middelfart Sparekasse.

Den af sparekassen nævnte afgørelse fra Ankenævnet, 17/2020, adskiller sig væsentligt fra hændelsesforløbet i nærværende sag og i de ovenstående sager.

Hun befandt sig i en presset situation, og hendes efterfølgende tvivl om en eventuel svindel er uden betydning for den viden, som hun havde eller burde have haft under telefonsamtalen, hvor svindlen fandt sted.

Det bestrides, at der foreligger egen skyld som følge af, at hun først kontaktede sparekassen næste dag. Under alle omstændigheder forudsætter betydningen af en eventuel egen skyld, at sparekassen skal dokumentere, at en tidligere reaktion fra hende ville have medført et mindre tab. Sparekassen kan ikke dokumentere dette.

Sparekassen er som følge heraf forpligtet til at tilbageføre 173.400 kr. til hende med fradrag af enten 375 kr. eller 8.000 kr., jf. betalingslovens § 100, stk. 3, eller stk. 4.

**Middelfart Sparekasse** har til støtte for frifindespåstanden blandt andet anført, at klageren, henset til SMS'ernes ordlyd, handlede med forsæt i forbindelse med videregivelsen. Klageren er kognitivt velfungerende. Hun videregav SMS-koderne med forsæt og under forudsætninger, hvor hun burde have indset, at der var stor risiko for misbrug, hvorfor hun selv er forpligtet til at bære det fulde tab, jf. lov om betalinger § 100, stk. 5.

Phishing-begrebet som beskrevet i lovbemærkningerne til betalingslovens § 100, stk. 5, har ikke været tiltænkt at omfatte de tilfælde, hvor en kunde videregiver SMS-koder, som tydeligt angiver, at de aldrig må udleveres til andre. Phishing-begrebet er tiltænkt de tilfælde, hvor en person ved en fejl kommer til at videregive sine oplysninger via falske links, spammails eller falske hjemmesider, og hvor en kunde f.eks. med føje tror, at de indtaster deres kort- eller login-oplysninger på en rigtig hjemmeside, som efterfølgende viser sig at være falsk.

Nærværende sag, hvor klageren først videregav sine fortrolige oplysninger over telefonen og efterfølgende videregav seks SMS-koder, går langt ud over, hvad der var tiltænkt med phishing-begrebet i lovbemærkningerne særligt under hensyn til, at SMS-teksten tydeligt angav, at koden aldrig måtte udleveres til andre.

Hvis man ikke i sådanne tilfælde må anses for at have haft forsæt til videregivelsen og efterfølgende en burde-viden om risiko for misbrug, stiller sparekassen sig uforstående over for, hvilke yderligere sikkerhedsforanstaltninger, der skal indføres, førend kunde kan forpligtes til at bære tabet for egen manglende agtpågivenhed. Hvis § 100, stk. 5, ikke kan finde anvendelse i nærværende situation, åbnes der op for, at reglen kan misbruges af svindlere, som kan udnytte pengeinstitutternes ufravigelige forpligtelse til at dække tabet.

Herudover henvises til Ankenævnets principielle afgørelse, 17/2020, hvor Ankenævnet kom frem til, at § 100, stk. 5, fandt anvendelse på trods af, at af den forurettede var blevet udsat for phishing.

Klageren har i forbindelse med behandlingen af indsigelsessagen over for sparekassen oplyst, at hun i forbindelse med opkaldet fra M blev mistænksom og drøftede sagen med nogle bekendte på den festival, som hun opholdt sig, hvilket indikerer, at klageren havde en burde-viden om, at der var tale om svindel. Klageren forholdt sig passiv på trods af denne viden, idet hun ventede hele 20 timer med at kontakte sparekassen, hvilket indikerer, at hun ikke følte sig presset i situationen.

Middelfart Sparekasse har til støtte for afvisningspåstanden anført, at en yderligere afklaring af klagerens forsæt og burde-viden vil kræve en parts- og vidneforklaring, som medfører, at sagen ikke er egnet til behandling for Ankenævnet, hvorfor sagen bør afvises.

### **Ankenævnets bemærkninger**

Den 20. juni 2019 blev der via netbank foretaget seks overførsler (en overførsel på 13.000 kr., fire overførsler på 15.000 kr. og en overførsel på 250.000 kr.) på i alt 323.000 kr. fra klagerens konti i Middelfart Sparekasse til tredjemands konti i andre pengeinstitutter.

Baggrunden for overførslerne var, at klageren samme dag blev kontaktet telefonisk af en person, M, der udgav sig for at være fra Nets, og som oplyste, at klageren var under hackerangreb, hvilket M kunne afværge, hvis klageren videregav nogle oplysninger til ham. Klageren modtog samme dag i tidsrummet fra kl. 14:04 til 14:33 seks SMS'er. Klageren videregav sine NemID-oplysninger og SMS-koderne til M, der fik adgang til klagerens netbank.

Det lykkedes ifølge det oplyste sparekassen at få tilbageført 149.600 kr., og overførslerne fra klagerens konto udgjorde herefter 173.400 kr.

Transaktionerne skyldtes tredjemands misbrug af de af klageren videregivne oplysninger, herunder klagerens NemID-oplysninger. Det lægges 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 svingagtigt, eller at betaleren har undladt at opfylde sine forpligtelser, jf. betalingslovens § 93.

Ankenævnet finder, at klagerens NemID var en personlig sikkerhedsforanstaltning, jf. betalingsloven § 7, nr. 31.

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.

Det fremgår af forarbejderne til betalingslovens § 100, stk. 5, (lovforslag nr. L157, af 15. marts 2017), at hæftelse uden beløbsbegrænsning ikke finder anvendelse, hvis den personlige sikkerhedsforanstaltning uforvarende er overladt til andre, eksempelvis i forbindelse med phishing, idet betaleren ikke har overdraget den personlige sikkerhedsforanstaltning med forsæt til, at der skal foretages den uberettigede anvendelse.

Ankenævnet finder, at klageren har været udsat for phishing. Ankenævnet finder derfor, at sparekassen ikke 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.

I løbet af telefonsamtalen med M modtog klageren i alt seks SMS'er med engangskoder. Det fremgik af SMS'erne, at engangskoden skulle indtastes i netbank for at godkende en betaling, at koden aldrig måtte udleveres til andre, og at hun skulle kontakte sit pengeinstitut og/eller spærre sit NemID, hvis hun ikke var i gang med en betaling. På trods af dette videregav klageren engangskoderne til M. Ankenævnet finder, at klageren ved at videregive sine NemID-oplysninger og engangskoderne til M har udvist groft uforsvarlig adfærd, og at klageren som følge heraf hæfter med op til 8.000 kr. Det gælder, selv om det som anført må lægges til grund, at hun har været udsat for phishing.

Middelfart Sparekasse skal derfor tilbageføre differencen på 165.400 kr. til klagerens konti med valør fra datoen for debiteringerne.

#### **Ankenævnets afgørelse**

Middelfart Sparekasse skal inden 30 dage tilbageføre 165.400 kr. til klagerens konti med valør fra datoen for debiteringerne.

Klageren får klagegebyret tilbage.