VESTRE LANDSRET
DOM
afsagt den 9. december 2022

Sag BS-2380/2022-VLR
(9. afdeling)

B.
(advokat Tinne Drejer Steffensen)

mod

Middelfart Sparekasse
(advokat Janus Winther Høy)

Landsdommerne Cecilie Kabel Revsbech, Mogens Heinsen og Mette Hartmann Andresen (kst.) har deltaget i sagens afgørelse.

Sagen er anlagt ved Retten i Odense den 21. maj 2021.

Ved kendelse af 4. oktober 2021 fra Retten i Odense blev sagen henvist til behandling ved landsretten efter retsplejelovens § 226, stk. 1, og parterne aftalte herefter, at de ønskede sagen behandlet ved Vestre Landsret, jf. retsplejelovens § 245.

Sagen drejer sig om afgrænsningen mellem betalingslovens § 100, stk. 4, nr. 3, og betalingslovens § 100, stk. 5, herunder om sagsøgeren, B., alene har udvist en groft uforsvarlig adfærd, eller om B. med forsæt har videregivet oplysninger til tredjemand under omstændigheder, hvor hun indså eller burde have indset, at der var risiko for misbrug.

B. er af den opfattelse, at hændelsesforløbet er omfattet af betalingslovens § 100, stk. 4, nr. 3, mens sagsøgte, Middelfart Sparekasse, er af den opfattelse, at hændelsesforløbet er omfattet af betalingslovens § 100, stk. 5.

Påstande
B. har nedlagt påstand om, at Middelfart Sparekasse til hende skal betale 165.400,00 kr. med procesrente fra den 21. maj 2021 til betaling sker.

Middelfart Sparekasse har påstået frifindelse, subsidiært frifindelse mod betaling af et af retten fastsat mindre beløb.

Sagsfremstilling
B. var i juni 2019 kunde i Middelfart Sparekasse, hvor hun blandt andet havde en lønkonto (med et kontonummer, som endte på 420), en anden konto (med et kontonummer, som endte på 353) samt netbankadgang. Der blev den 20. juni 2019 hævet i alt 323.000 kr. fra B's konti. Det lykkedes Middelfart Sparekasse at få tilbageført 149.600 kr., men sparekas-sen afviste at tilbageføre tabet på 173.400 kr. til B., der den 29. juli 2020 indbragte sagen for Det finansielle ankenævn. Der er mellem parterne enighed om det faktiske forløb, der er beskrevet således i Det finansielle anke-nævns afgørelse af 5. marts 2021:

"…
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 hævninger 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 er 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 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.

…"

Af ankenævnets begrundelse fremgår:

"…

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 konto 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. betalings-lovens § 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 var en personlig sikkerhedsforanstaltning, jf. betalingslovens § 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.

…"

Middelfart Sparekasse meddelte den 11. marts 2021 Det finansielle ankenævn, at sparekassen ikke ønskede at være bundet af ankenævnets afgørelse.

Retsgrundlag
Der er enighed mellem parterne om, at spørgsmålet om, hvorvidt Middelfart Sparekasse er forpligtet til at tilbageføre det tabte beløb på 173.400 kr. med fradrag af det anerkendte beløb på 8.000 kr., skal afgøres efter § 100 i Lov om betalinger (nu lovbekendtgørelse nr. 2710 af 7. december 2021).

Lovens § 100 har følgende ordlyd:

> § 100
> Betalerens udbyder af betalingstjenester hæfter i forhold til betaleren for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af stk. 2-5. Betaleren hæfter kun efter stk. 3-5, hvis transaktionen er korrekt registreret og bogført, jf. dog stk. 2.
>
> Stk. 2.
> Betaleren hæfter uden beløbsbegrænsning for tab, der opstår, som følge af at betaleren har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter § 93.

Stk. 3.
Medmindre videregående hæftelse følger af stk. 4 og 5, hæfter betaleren med op til 375 kr. for tab som følge af andres uberettigede anvendelse af betalingstjenesten, hvis den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt.

Stk. 4.
Medmindre videregående hæftelse følger af stk. 5, hæfter betaleren med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingstjenesten, hvis betalerens udbyder godtgør, at den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, og

1) at betaleren har undladt at underrette betalerens udbyder snarest muligt efter at have fået kendskab til, at det til betalingstjenesten hørende betalingsinstrument er bortkommet eller den personlige sikkerhedsforanstaltning er kommet til den uberettigedes kendskab,
2) 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
3) at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

Stk. 5.
Betaleren hæfter 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.

Stk. 6.
Uanset stk. 3-5 hæfter betalerens udbyder for uberettiget anvendelse, der finder sted,

1) efter at udbyderen har fået underretning om, at det til betalingstjenesten hørende betalingsinstrument er bortkommet, at en uberettiget person har fået kendskab til den personlige sikkerhedsforanstaltning, eller at betaleren af andre grunde ønsker betalingsinstrumentet spærret,
2) når det er forårsaget af handlinger, der er foretaget af en udbyders ansatte, agent eller filial eller en enhed, hvortil udbyderens aktiviteter er outsourcet, eller disses passivitet, eller

3) fordi udbyderen ikke har truffet egnede foranstaltninger, jf. § 94, stk. 1, nr. 2.

Stk. 7.
Uanset stk. 3-5 hæfter betalerens udbyder tillige, hvis udbyderen ikke kræver stærk kundeautentifikation, medmindre betaleren har handlet svigagtigt. Betalingsmodtageren eller dennes udbyder skal godtgøre de tab, der er påført betalerens udbyder, hvis betalingsmodtageren eller dennes udbyder har undladt at anvende stærk kundeautentifikation. 1. og 2. pkt. finder ikke anvendelse på tjenester omfattet af § 1, stk. 5, og § 5, nr. 14-16.

Stk. 8.
Uanset stk. 3-5 hæfter betalerens udbyder tillige, hvis tabet, tyveriet eller den uberettigede tilegnelse af det til betalingstjenesten hørende betalingsinstrument eller den til betalingstjenesten hørende personlige sikkerhedsforanstaltning ikke kunne opdages af betaleren forud for den uberettigede anvendelse.

Stk. 9.
Uanset stk. 3-5 hæfter betalerens udbyder tillige, hvis betalingsmodtageren vidste eller burde vide, at der forelå en uberettiget anvendelse af betalingstjenesten.

Stk. 10.
Stk. 1-9 finder tillige anvendelse på elektroniske penge, medmindre det ikke er muligt for betalerens udsteder af elektroniske penge at spærre betalingskontoen eller betalingsinstrumentet.

Forslag til lov om betalinger (betalingsloven), L 157, blev fremsat den 15. marts 2017 og skulle erstatte den gældende lov om betalingstjenester og elektroniske penge (lovbekendtgørelse nr. 613 af 24. april 2015) og gennemføre Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked (2. betalingstjenestedirektiv), samt Europa-Parlamentets og Rådets direktiv 2009/110/EU af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed (2. e-pengedirektiv) i dansk ret. Af de almindelige bemærkninger til lovforslaget (FT 2016-17, tillæg A, L 157, side 42 ff.) fremgår bl.a.:

"…

Den nugældende lov om betalingstjenester og elektroniske penge blev vedtaget i 2009. Siden da er der sket store teknologiske fremskridt på it-

området, som har gjort det muligt at udvikle nye online og mobile betalingsløsninger, som der ikke var tænkt på under tilblivelse af den nugældende lov. Mange nye betalingstjenester falder derfor slet ikke, eller kun i mindre grad, ind under anvendelsesområdet for den nugældende lov. Som følge af udviklingen på området har der været et behov for at håndtere nye sikkerhedsrisici og en manglende forbrugerbeskyttelse på visse områder.

Lovforslagets hovedformål er at sikre, at rammerne for udbuddet af elektroniske betalingstjenester fortsat er tidssvarende og reflekterer den teknologiske udvikling. Med lovforslaget fastsættes nye regler, der vil give en klarere retsstilling og sikre ensartede vilkår for alle udbydere af betalingstjenester…

…

Lovforslaget sikrer endvidere mere gennemsigtighed og åbenhed omkring betingelserne for brugen af betalingstjenester ved at fastsætte en række oplysningskrav for udbydere af betalingstjenester i forbindelse med udbud og brug af en betalingstjeneste. Derudover sikrer lovforslaget, at brugerne er tilstrækkeligt sikret i tilfælde af misbrug, uafhængigt af, hvilken type af betalingstjeneste, der anvendes.

…

Den gældende lov om betalingstjenester og elektroniske penge regulerer også hvilke ansvars- og hæftelsesregler, der gælder i forbindelse med uautoriserede betalingstransaktioner. Loven tilsiger, at det som udgangspunkt er udbyder, som hæfter som følge af uautoriserede betalingstransaktioner. En bruger hæfter dog for op til 1.200 kroner, for andres uberettigede anvendelse af betalingsinstrumentet i tilfælde, hvor den personlige sikkerhedsforanstaltning, såsom PIN-koden, er anvendt. For helt særlige tilfælde, hvor en bruger har undladt at underrette udbyderen efter at være blevet bekendt med, at betalingsinstrumentet var stjålet, eller at sikkerhedsforanstaltningerne var kommet til andres uberettigede kendskab, hæfter brugeren for op til 8.000 kroner for andres uberettigede brug. Endelig hæfter brugeren ubegrænset i tilfælde, hvor denne har handlet med forsæt, eller hvis denne har oplyst sin personlige sikkerhedsforanstaltninger til den, som har foretaget misbruget, og brugeren burde have vidst eller indset, at der var risiko for misbrug. Loven fastsætter endvidere regler om, at en bruger skal foretage indsigelse mod en uautoriseret betalingstransaktion snarest og senest 13 måneder efter, midlerne er debiteret kontoen.

…"

Af de specielle bemærkninger til lovforslaget (FT 2016-17, tillæg A, L 157, side 236 ff.) fremgår bl.a. om § 100:

> "…
>
> Det følger af § 62 i den nugældende lov om betalingstjenester og elektroniske penge, at betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af et betalingsinstrument, medmindre andet følger af stk. 2-6. Betaler hæfter kun efter stk. 2-6, hvis transaktionen er korrekt registreret og bogført. Ved en uberettiget anvendelse af et betalingsinstrument skal betalers udbyder straks tilbagebetale betaleren beløbet. Betaleren hæfter dog uden beløbsbegrænsning for tab, der opstår som følge af, at betaler har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter § 59.
>
> Forslaget til § 100 fastlægger den ansvarsfordeling, som skal gælde, hvis et betalingsinstrument bruges af en person, som ikke er berettiget til at bruge det.
>
> Den foreslåede bestemmelse viderefører med visse indholdsmæssige ændringer § 62 i den nugældende lov om betalingstjenester og elektroniske penge. Bestemmelsen gennemfører artikel 74, i 2. betalingstjenestedirektiv. Idet det dog følger af artikel 74, 4. pkt., i 2. betalingstjenestedirektiv, at medlemslandene kan fastsætte andre hæftelses- og ansvarsregler for betaleren, hvis denne hverken har optrådt svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser i henhold til artikel 69 i 2. betalingstjenestedirektiv, der er gennemført i dette lovforslags § 93.
>
> Det er således hensigten med forslaget til § 100 at videreføre eksisterende praksis vedrørende hæftelses- og ansvarsreglerne i forbindelse med uberettigede anvendelse af en betalingstjeneste, dog med de to ændringer, der følger af 2. betalingstjenestedirektiv. Med disse to ændringer indføres to nye ansvarsnormer, idet betaler ifølge 2. betalingstjenestedirektiv ikke hæfter for tab, såfremt betalerens udbyder ikke kræver stærk kundeautentifikation, medmindre betaleren har handlet svigagtigt, eller hvis betaler ikke med rimelighed kunne opdage tabet, tyveriet eller den uberettigede tilegnelse af det til betalingstjenesten hørende betalingsinstrument eller personlige sikkerhedsforanstaltning forud for den uberettigede anvendelse.
>
> Det foreslås i stk. 1, 1. pkt., at betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af stk. 2-5.

Med bestemmelsen fastslås, at der gælder en grundlæggende regel om, at betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af stk. 2-5.

…

Det foreslås i stk. 4, at medmindre videregående hæftelse følger af stk. 5, hæfter betaleren med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingstjenesten, hvis betalers udbyder godtgør, at den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, og 1) at betaleren har undladt at underrette betalers udbyder snarest muligt efter at have fået kendskab til, at det til betalingstjenesten hørende betalingsinstrument er bortkommet, eller at den personlige sikkerhedsforanstaltning er kommet til den uberettigedes kendskab, 2) at betaleren med forsæt har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 4, eller 3) at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

§ 100, stk. 4, omhandler de tilfælde, hvor den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, eksempelvis en pinkode eller en enhed til generering af engangskoder, og betaler samtidig har udvist en adfærd, der har muliggjort den uberettigede anvendelse, uden at yderligere hæftelse følger af stk. 5.

Forslaget til stk. 4, skal læses i sammenhæng med forslaget til stk. 7, som gennemfører artikel 74, stk. 2, i 2. betalingstjenestedirektiv, hvorefter betaleren ikke bærer nogen økonomiske tab, såfremt betalerens udbyder ikke kræver stærk kundeautentifikation, medmindre betaleren har handlet svigagtigt. Ifølge forslaget til stk. 7, 3. pkt. vil betaler dog i visse tilfælde kunne hæfte for eventuelle tab, når den personlige sikkerhedsforanstaltning har været anvendt, selvom betalers udbyder ikke kræver stærk kundeautentifikation, da der for enkelte typer af tjenester ikke er krav om anvendelse af stærk kundeautentifikation.

De tilfælde i stk. 4, nr. 1-3, hvor brugeren hæfter, omhandler alene brugerens manglende påpasselighed ved omgangen med den personlige sikkerhedsforanstaltning. Bestemmelsen understøtter herved, at der er tale om en personlig sikkerhedsforanstaltning, som ikke må overdrages til andre. Dette berører dog ikke brugerens mulighed for at anvende betalingsinitieringstjenester og kontooplysningstjenester. Bestemmelsen indeholder derfor ikke udtrykkelige regler om, hvorledes en anden person skal agere,

hvis denne person har fået overdraget sikkerhedsforanstaltningen af brugeren, og hvis sikkerhedsforanstaltningen i en sådan situation kompromitteres.

Hvis der er knyttet en personlig sikkerhedsforanstaltning til en betalingstjeneste, er det af afgørende betydning for at hindre andres uberettigede brug af betalingsinstrumentet, at denne behandles fortroligt og ikke røbes for andre. Den personlige sikkerhedsforanstaltning er således nøglen til benyttelsen af betalingstjenesten.

Brugeren må derfor ikke overlade eller oplyse denne sikkerhedsforanstaltning til andre, jf. lovforslagets § 93.

I tilfælde, hvor betaler uforvarende har overladt den personlige sikkerhedsforanstaltning til andre, eksempelvis i forbindelse med phishing, finder forslaget til stk. 4, nr. 2, dog ikke anvendelse, idet betaler ikke overdrog den personlige sikkerhedsforanstaltning med forsæt til, at der skal foretages den uberettigede anvendelse.

Det foreslås i stk. 5, at betaleren hæfter 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 betalers 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.

Med stk. 5 fastslås det, at betaleren hæfter ubegrænset for tab, der opstår som følge af andres uberettigede anvendelse af betalingsinstrumentet, såfremt den til betalingstjenesten hørende personlige sikkerheds foranstaltning har været anvendt, og betalerens udbyder kan godtgøre, at betaleren har oplyst den personlige sikkerhedsforanstaltning til den person, som har foretaget den uberettigede anvendelse, og betaleren har indset eller burde have indset, at der var risiko for misbrug.

Bestemmelsen understreger, at betaleren selv hæfter for tab, der opstår ved, at betaleren ved groft uforsvarlig adfærd eller bedrageri har muliggjort den uberettigede anvendelse. Det er dog en forudsætning, at betaler med forsæt har oplyst den personlige sikkerhedsforanstaltning, der anvendes til at foretage stærk kundeautentifikation. I tilfælde, hvor betaler uforvarende har overladt den personlige sikkerhedsforanstaltning til andre, eksempelvis i forbindelse med phishing, hæfter betaler ikke efter for-

slaget til stk. 5, idet betaler ikke overdrog den personlige sikkerhedsforanstaltning med forsæt på at der skal foretages den uberettigede anvendelse.

Forslaget til stk. 5, skal læses i sammenhæng med forslaget til stk. 7, som gennemfører artikel 74, stk. 2, i 2. betalingstjenestedirektiv, hvorefter betaleren ikke bærer noget økonomiske tab, såfremt betalerens udbyder ikke kræver stærk kundeautentifikation, medmindre betaleren har handlet svigagtigt. Ifølge forslaget til stk. 7, 3. pkt., vil betaler dog i visse tilfælde kunne hæfte for eventuelle tab, når den personlige sikkerhedsforanstaltning har været anvendt, selvom betalers udbyder ikke kræver stærk kundeautentifikation, da der for enkelte typer af tjenester ikke er krav om anvendelse af stærk kundeautentifikation.

…"

Anbringender
B. har til støtte for sin påstand bl.a. anført, at det fremgår af betalingslovens § 6, at loven i forhold til forbrugere er beskyttelsespræceptiv. Betalingslovens § 100 indeholder forskellige gradueringer i ansvarsfordelingen mellem udbydere og betalere (NemID-indehavere) i tilfælde af tab som følge af tredjemands uberettigede anvendelse af en betalingstjeneste.

Hovedreglen er, at udbyder af betalingstjenesten hæfter i forhold til betaleren for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, jf. betalingslovens § 100, stk. 1. Det fremgår af forarbejderne, at betalingsloven skal sikre, at brugere er tilstrækkeligt sikret i tilfælde af misbrug, uafhængigt af hvilken type betalingstjeneste der anvendes, og at betalerens udbyder hæfter i forhold til betaleren for tab som følge af andres uberettigede anvendelse af en betalingstjeneste. Forarbejderne fastslår, at betalingslovens § 100, stk. 4 og 5 omhandler de tilfælde, hvor den til betalingstjenesten hørende sikkerhedsforanstaltning har været anvendt, og fastslår videre, at uanset om et forhold er omfattet af stk. 4 eller 5, skal der anvendes en særlig forståelse af forsætsbegrebet, eksempelvis i forbindelse med phishing, idet forarbejderne fastslår, at betaleren ikke alene skal have handlet forsætligt ved udlevering af den personlige sikkerhedsforanstaltning, men at betaleren ved overdragelse af den personlige sikkerhedsforanstaltning skal have handlet med forsæt til, at der foretages den uberettigede anvendelse.

Betalingslovens § 100, stk. 5, finder ikke anvendelse i denne sag, idet bestemmelsen alene finder anvendelse, hvis betalerens udbyder godtgør, at betaleren med forsæt til, at der skulle foretages den uberettigede anvendelse, har oplyst sine personlige sikkerhedsforanstaltninger. Det er Middelfart Sparekasse, der har bevisbyrden for dette, og denne bevisbyrde har sparekassen ikke løftet.

B. har ikke handlet forsætligt i den forstand, at B. ikke med forsæt har overdraget sine personlige sikkerhedsforanstaltninger med forsæt til, at der skulle foretages den uberettigede anvendelse. B. har været udsat for phishing, sådan som Det finansielle ankenævn også har fastslået i sin afgørelse. Det er den almindelige samfundsmæssige opfattelse af, om et forhold, som det B. har været udsat for, er phishing, der finder anvendelse ved vurderingen af, hvorvidt forholdet er phishing.

Der er ingen retspraksis, som fastlægger fortolkningen og rækkevidden af betalingslovens § 100, stk. 4 og 5, men der findes en righoldig praksis fra Det finansielle ankenævn. Det finansielle ankenævn følger B.'s fortolkning af betalingslovens § 100, stk. 4 og 5, ligesom Det finansielle ankenævn i afgørelserne henviser til forarbejderne i betalingsloven. Det fremgår derudover af praksis fra Det finansielle ankenævn, at ankenævnet lægger vægt på, om betaleren var i en presset situation eller ikke. I de tilfælde, hvor ankenævnet fandt, at betaleren var i en presset situation, blev betaleren ikke pålagt at hæfte, jf. betalingslovens § 100, stk. 5. I disse tilfælde fandt ankenævnet, at forholdene var omfattet af betalingslovens § 100, stk. 4, idet betaleren havde udvist groft uforsvarlig adfærd, jf. afgørelserne 221/2021, 210/2021 og 402/2020. I de tilfælde, hvor Det finansielle ankenævn fandt, at betaleren ikke havde været i en presset situation, måtte betaleren selv hæfte for det tab, som betaleren havde lidt som følge af uberettiget anvendelse af en betalingstjeneste, jf. afgørelserne 17/2020 og 373/2019. Det finansielle ankenævn fastslår endvidere, at betaleren har været udsat for phishing i de tilfælde, hvor betaleren ved telefonisk henvendelse er blevet franarret sin personlige sikkerhedsforanstaltning, jf. afgørelserne 221/2021, 210/2021 og 402/2020. Det finansielle ankenævns praksis er i overensstemmelse med betalingslovens ordlyd og forarbejder og er derfor korrekt. Forarbejderne til betalingslovens § 100, stk. 5, anfører alene phishing som et eksempel, idet definitionen ikke er udtømmende.

B. har ikke tilsidesat sin tabsbegrænsningspligt. Middelfart Sparekasse har under alle omstændigheder ikke dokumenteret, at en hurtigere reaktion fra B. kunne have reduceret tabet.

Middelfart Sparekasse har til støtte for sine påstande bl.a. anført, at sparekassen har godtgjort, at B. indså eller burde have indset, at videre-givelsen af en række oplysninger til tredjemand medførte risiko for misbrug, herunder at oplysningerne er videregivet med forsæt (med viden og med vil-je/frivilligt), hvorefter betalingslovens § 100, stk. 5, finder anvendelse.

Der findes forskellige former for bedrageri, som it-kriminelle kan anvende over for en person for at narre denne til at udlevere sine personlige betalingsoplysninger, herunder phishing, smishing og vishing. I denne sag er der ikke tale om phishing, sådan som phishingbegrebet er defineret i betalingsloven, idet phis-

hingbegrebet i lovforslag 2016-17 L 157 er defineret som det forhold, at en person "uforvarende" har overladt den personlige sikkerhedsforanstaltning til andre. I denne sag har B. frivilligt og med viden afgivet de per-sonlige sikkerhedsforanstaltninger i form af adgangskode, brugernavn og NemID nøgle samt efterfølgende 6 SMS-koder, der efter deres ordlyd ikke måtte udleveres til andre, til tredjemand. Der er derfor ikke tale om en "uforvarende" videregivelse svarende til den, forarbejderne definerer som phishing, og betalingslovens § 100, stk. 5, finder derfor anvendelse, hvorefter B. hæfter for det fulde beløb.

Såfremt landsretten finder, at B. har været udsat for phishing, er det Middelfart Sparekasses opfattelse, at lovbemærkningerne vedrører én type af phishing, og at der ikke heri er taget højde for andre typer af phishing, såkaldt "social engineering" eller "vishing", som denne sag vedrører. Lovens forarbejder er alene tiltænkt anvendt i den klassiske phishing-situation, hvor en person modtager en e-mail, angiveligt fra en pålidelig afsender, og bliver bedt om at indtaste en række oplysninger, som herefter bliver misbrugt. I en sådan situation er oplysningerne ikke givet forsætligt, idet den besvegne slet ikke er vidende om, at denne videregiver sine oplysninger til tredjemand, men i stedet tror, at denne indtaster sine oplysninger på en legitim hjemmeside, og lovens forarbejder giver alene her mening. Lovens forarbejder kan derimod ikke meningsfuldt være møntet på den situation, hvor en person over telefonen helt bevidst udleverer sin adgangskode, sit brugernavn, samt NemID-nøgle og efterfølgende 6 SMS-koder til tredjemand, da personen her ved, at oplysningerne udleveres til tredjemand. Der er ikke i denne situation tale om en uforvarende eller ikke-forsætlig videregivelse, og der er således ikke tale om phishing i betalingslovens forstand. Det centrale er, hvorledes lovgiver har forstået phishingbegrebet på tidspunktet for lovforarbejdernes udarbejdelse og ikke den samfundsmæssige opfattelse af phishing. Lovens forarbejder kan derfor ikke anvendes på den i denne sag foreliggende situation.

Såfremt landsretten finder, at lovforarbejderne kan anvendes i den i sagen foreliggende situation, gøres det gældende, at antagelsen i forarbejderne om, at betaleren ikke kan hæfte med mere end op til 8.000 kr., jf. betalingslovens § 100, stk. 4, nr. 3, hvis vedkommende har været udsat for phishing, da betaleren ved denne type misbrug må antages at have overladt den personlige sikkerhedsforanstaltning uforvarende til misbrugeren, ikke er korrekt. Det er ikke korrekt, at betaleren i alle phishing-situationer overlader sine oplysninger uforvarende. Betaleren lokkes således ved vishing netop til at udlevere sine oplysninger til tredjemand med fuldt overlæg (forsæt). Endvidere giver det ikke mening at lade forsætskravet relatere sig til den uberettigede anvendelse.

En sædvanlig ordlydsfortolkning af betalingslovens § 100, stk. 5, må føre til, at det afgørende er, om betaleren har haft forsæt til at udlevere oplysningerne til

tredjemand. Hvis betaler selv havde forsæt til misbruget, er forholdet utvivlsomt omfattet af betalingslovens § 100, stk. 2, og dermed ville betaleren hæfte for hele tabet og medvirke til en strafbar handling. Hvis forsætskravet skulle forstås som en henvisning til forsæt til misbruget, ville betalingslovens § 100, stk. 3-5, være overflødig ved phishing som i denne sag.

Derfor er det, som landsretten reelt skal vurdere i denne sag, en fortolkning af betalingslovens § 100, stk. 5, sidste led, hvorefter det skal vurderes, om videregivelsen er sket under omstændigheder, hvor B. indså eller burde have indset, at der var risiko for misbrug. En sådan vurdering vil navnlig på baggrund af de modtagne SMS'er og det forhold, at oplysningerne er vide-regivet med forsæt (viden og med vilje/frivilligt), resultere i, at B. indså eller burde have indset, at videregivelsen medførte risiko for misbrug, hvorefter betalingslovens § 100, stk. 5, finder anvendelse.

Hvis en situation som denne kategoriseres som phishing samtidig med, at forsætsbegrebet ikke kan finde anvendelse ved phishing, er der reelt tale om et objektivt ansvar eller en objektiv hæftelse for pengeinstitutter i forhold til betaling ved svindel, hvilket ikke er formålet med loven og imod lovens ordlyd.

Middelfart Sparekasses fortolkning af betalingslovens § 100, stk. 5, har støtte i praksis fra Det finansielle ankenævn, herunder særligt afgørelse 17/2020, hvor ankenævnet fandt, at betalingslovens § 100, stk. 5, fandt anvendelse, selvom der var tale om phishing, og ankenævnet gik dermed direkte imod forarbejderne til betalingsloven. Afgørelsen illustrerer, at betalingslovens § 100, stk. 5, til trods for lovens forarbejder godt kan finde anvendelse i phishing-situationer.

B. har ikke opfyldt sin tabsbegrænsningspligt, idet hun ikke, så snart hun var blevet bekendt med misbruget, underrettede Middelfart Spare-kasse herom. B. undlod således i en periode på 16 timer, efter at hun var blevet mistænksom, at underrette Middelfart Sparekasse om misbruget og undlod at spærre sit dankort. Havde B. opfyldt sin under-retningspligt, kunne alle de uretmæssige betalinger være hindret, og B. hæfter derfor også af denne grund for det fulde beløb.

Landsrettens begrundelse og resultat
Der er mellem parterne enighed om, at der den 20. juni 2019 via netbank blev foretaget 6 uberettigede overførsler på i alt 323.000 kr. fra B. konti i Middelfart Sparekasse til tredjemands konti i andre pengeinstitutter, og at det efterfølgende lykkedes Middelfart Sparekasse at få tilbageført 149.600 kr. således, at de uberettigede overførsler fra B.'s konti herefter udgør 173.400 kr.

Der er endvidere enighed om, at baggrunden for overførslerne var, at B. samme dag var blevet kontaktet telefonisk af en person, der udgav sig for at være fra Nets, og som oplyste, at B. var under hackerangreb, hvilket personen kunne afværge, hvis B. videregav oplys-ninger til ham i form af CPR-nummer, personlig kode, NemID-nøglekode og efterfølgende 6 SMS-koder, modtaget samme dag inden for 30 minutter. B., der på internettet havde søgt og fundet navnet, som personen havde angivet, videregav oplysningerne, hvorefter personen fik adgang til B.'s netbank.

Landsretten finder efter det ovenfor anførte, at B. har været udsat for phishing eller en adfærd, som må sidestilles hermed. Desuagtet har B. frivilligt, bevidst og forsætligt overladt sine NemID-oplysninger og SMS-koder til tredjemand, og betalingslovens § 100, stk. 5, finder derfor efter sin ordlyd anvendelse, hvis bestemmelsens betingelser i øvrigt er til stede, idet det, som bestemmelsen er formuleret, ikke er et krav, at B. også har haft forsæt til, at der foretages den uberettigede anvendelse.

Det afgørende er herefter, om B. har oplyst sine NemID-oplysninger og SMS-koder til tredjemand under omstændigheder, hvor hun – på det tidspunkt – indså eller burde indse, at der var en risiko for misbrug.

Formålet med betalingsloven var blandt andet at sikre, at brugerne er tilstrækkeligt sikret i tilfælde af misbrug, uafhængigt af hvilken type af betalingstjeneste, der anvendes, og betalingslovens § 100, stk. 1, hvorefter det som udgangspunkt er betalerens udbyder af betalingstjenester, der hæfter for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, er i overensstemmelse hermed.

Der må herefter kræves en høj grad af uagtsomhed ved bedømmelsen af, om en betaler indså eller burde have indset, at der var risiko for misbrug på det tidspunkt, hvor den til betalingstjenesten hørende personlige sikkerhedsforanstaltning blev oplyst til tredjemand.

Landsretten finder, at Middelfart Sparekasse ikke har godtgjort, at B. har oplyst sine NemID-oplysninger og SMS-koder til tredjemand under omstændigheder, hvor hun indså eller burde have indset, at der var en risiko for misbrug, herunder at tredjemand ikke ville handle i hendes interesse, og betalingslovens § 100, stk. 5, finder derfor ikke anvendelse.

B. hæfter således ikke efter betalingslovens § 100, stk. 5, uden beløbsbegrænsning for det tab, der opstod som følge af den uberettigede anvendelse af betalingstjenesten. B. har derimod ikke bestridt, at

hun i medfør af betalingslovens § 100, stk. 4, nr. 3, hæfter for et beløb på 8.000 kr., hvilket er fratrukket i den nedlagte påstand.

Endvidere finder landsretten ikke, at det er godtgjort, at B. har tilsidesat sin tabsbegrænsningspligt, herunder at det ville have ført til et mindre tab, såfremt B. havde kontaktet Middelfart Sparekasse på et tidligere tidspunkt.

Landsretten tager derfor B. påstand til følge.

Efter sagens udfald skal Middelfart Sparekasse i sagsomkostninger betale 49.260 kr. til B. 45.000 kr. af beløbet er til dækning af udgifter til advokatbistand inkl. moms og 4.260 kr. til retsafgift. Ud over sagens værdi er der ved fastsættelsen af beløbet til advokat taget hensyn til sagens omfang og forløb samt sagens principielle betydning.

THI KENDES FOR RET:

Middelfart Sparekasse skal inden 14 dage til B. betale 165.400 kr. med procesrente fra den 21. maj 2021, og sagsomkostninger med 49.260 kr.

Sagsomkostningerne forrentes efter rentelovens § 8 a.

Publiceret til portalen d. 09-12-2022 kl. 10:00
Modtagere: Sagsøger B., Sagsøgte Middelfart Sparekasse