RETTEN I VIBORG
DOM

afsagt den 2. maj 2025

Sag BS-33512/2024-VIB

S1

(advokat Mikkel Nielsen)

mod

BALLING SPAREKASSE (v. Jakob Jeldtoft)

Denne afgørelse er truffet af dommer Bybjerg Nielsen.

Sagens baggrund og parternes påstande
Retten har modtaget sagen den 2. juli 2024.

Sagen drejer sig om , S1s, indsigelse mod at hæfte for netbankoverførsler, der blev foretaget fra hendes konto i forbindelse med telefonopkald fra ukendt trediemand.

S1 har nedlagt følgende påstand:
Principalt: Sagsøgte tilpligtes at betale kr. 161.625 med tillæg af procesrente fra sagens anlæg.
Subsidiært: Sagsøgte tilpligtes at betale kr. 154.000 med tillæg af procesrente fra sagens anlæg.

BALLING SPAREKASSE har nedlagt følgende påstand
Principalt: Frifindelse
Subsidiært: Sagen afgøres efter lov om betalinger (LBK nr 53 af 18/01/2023) § 100, stk. 5.

Oplysningerne i sagen

Det påstævnte beløb udgør summen af 6 netbankoverførsler på i alt 162..000 kr., foretaget fra S1s konto hos Balling Sparekasse i perioden fra den 13. til den 23. december 2022, nærmere bestemt således:

- Den 13. december 2022 45.000 kr.
- Den 19. december 2022 50.000 kr.,
- Den 23. december 2022 10.000 kr., 10.000 kr., 46.000 kr. og 1.000 kr.

Overførslerne skete til tredjemands konti i andre pengeinstitutter.

I den principale påstand er de hævede beløb fratrukket en selvrisiko på 375 kr., mens der i den subsidiære påstand er fratrukket en selvrisiko på 8.000 kr.

Det er oplyst, at S1 efter egen anmodning er umyndiggjort den 31. juli 2023.

Det fremgår, at sagen har været forelagt Det Finansielle Ankenævn.

Af nævnets afgørelse, der er truffet den 28. februar 2024 fremgår af sagsfremstillingen bl.a.:

> "…
> Klageren var kunde i Sparekassen Balling, hvor hun havde konti og adgang til netbank.
>
> I perioden fra den 13. til den 23. december 2022 blev der foretaget seks netbankoverførsler på i alt 162.000 kr. fra klagerens konti til tredjemands konti i andre pengeinstitutter, tre overførsler indbetalt til klagerens konti på i alt 107.253,54 kr. (50.000 kr., 21.000 kr. og 36.253,54 kr.) samt to korttransaktioner i EUR til to kryptovalutabørser, som klageren ikke kan vedkende sig. Af kontoudskrift fremgår to kortbetalinger på henholdsvis 450 EUR og 100 EUR.
>
> Sparekassen har vedrørende de tre overførsler til klagerens konti oplyst, at to af overførslerne var udbetaling af provenu af nogle lån optaget i klagerens navn i to pengeinstitutter, PI og P2, og at den tredje overførsel på 36.253,54 kr. var en tilbageførsel/returnering fra pengeinstituttet P3 til klageren i forbindelse med en netbankoverførsel fra klagerens konto.
>
> Om baggrunden for transaktionerne har klageren oplyst, at hun over længere tid var blevet kontaktet telefonisk af en svindler, S, der udgav sig for at være fra et investeringsfirma, som skulle lukke nogle bitcoinkonti. S oplyste, at klageren havde mange tusinde kroner stående på en lille bitcoininvestering, som klageren havde udført. Hvis klageren samarbejdede med S, vi1le hun få disse penge udbeta1t. S pressede hende til at installere et

fjernstyringsprogram på både hendes PC og telefon under påskud af at ville hjælpe hende.

Sparekassen har oplyst, at transaktionerne er korrekt registreret og bogført og ikke er ramt af tekniske svigt eller andre fejl, og at de blev godkendt via MitlD-app og ved engangskode sendt pr. SMS til klagerens telefonnummer.

Klageren har anført, at hun ikke modtog sådanne SMS'er, og at hun ikke godkendte transaktionerne.

Sparekassen har fremlagt en transskription af klagerens (K) samtaler med sparekassen (R) den 23. og 29. december 2022 samt den 4. og 20. februar 2023, hvoraf det blandt andet fremgår:

Samtale den 23. december 2022
"... R: Nå K, jeg har lige talt med vores support. Det er lidt noget rod.
K: Meget rod, det kan vi godt blive enige om.
R: Ja, fordi umiddelbart har du optaget lån for 100.000. Kan det passe?
K: Det håber jeg ikke da.
R: Det er jo gået nogle penge ind.
K: Ja det er jo det.
R: Ja. Du har politianmeldt det ikke?
K: Nej, men det gør jeg. Det sagde hun (red: medarbejder fra Sparekassen) at jeg skulle gøre. ...
K: Jeg er fuldstændig enig med dig i det er noget rod
R: har det været uoverskueligt med det der kort? Eller hvordan? Har du brug for hjælp til noget?
K: Dumhed, tror jeg. Det er dyrt at være fattig. Så falder man jo for alt muligt mærkeligt.
R: Altså de der 50.000, det er noget du troede du investerede i noget?
K: Øh nej, det var det ikke.

Samtale den 29. december 2022:
"... R: Vi er jo også blevet kontaktet af [P3] med de der penge du har overført blandt andet. Har du det der overblik over hvad du har taget af lån?
K: Nej det har jeg simpelthen ikke.
R: Men du har politianmeldt det?
K: Ja det sagde hun jo jeg skulle. ..."

Samtale den 3. februar 2023:
" ...
R: Der står 36.000 på en opsparing. Det er jo dem de nåede at stoppe. ...
R: Det er jo nogen af de penge, som du har været i sving med at overføre rundt omkring. Der var nogle af de ting jo blevet stoppet. Og blandt andet det der ja. ...

K: og så snakkede du om at du kunne se at der var lån i op til 17 banker. Hvordan ved du det?
R: Jamen det sagde du jo selv.
K: Nej jeg sagde 12
R: Nej du sagde 17, da du var herinde. Men det du skal gøre er, når din årsopgørelse fra skat kommer, altså alt andet lige vil de jo også begynde at komme med noget opkrævning til dig. Er der begyndt at komme nogen af dem?
K: Ja der er så. Men det er de to banker i bad mig kontakte.
..."

Samtale den 20. februar 2023:
"... R: Det der du havde sendt. Skal du bare have mundtlig svar på det?
K: Nej jeg vil gerne have et skriftligt svar, da min hukommelse er en si. Som jeg skrev også i en mail
R: men vi er stadigvæk enige om, at du har overført?
K: Nej det har jeg ikke.
R: Men du har jo fået sms'er om at du skal godkende beløbene før transaktionen sker
K: Nej det har jeg ikke.
R: Men du har vel overladt dit Nemid til andre, så de kunne låne pengene?
K: Jaja det har jeg godkendt....
R: Men du kan jo ikke overføre så store beløb uden at få en SMSgodkendelse.
K: Jamen det har jeg ikke fået
R: Siger du at du aldrig har fået sms godkendelse, når der er overført penge herfra?
K: Jeg har markeret de beløb jeg ikke vil vedkende mig med markpen, så kan du lige tage dem med til juridisk afdeling
R: Du siger du ikke, at du ikke kender til dem? Altså du siger på tro og love at du ikke har fået nogen sms'er på det?
K: Ja at der skulle hæves nogle penge ja.
R: Men du har jo erkendt at du godt vil låne nogle penge til og investere for. Havde du ikke?
K: Sådan er det ikke foregået, R.
R: Jamen det sagde du da dengang du snakkede med mig. Hende damen du talte med havde overtalt dig til at investere nogle penge i forskellige investeringsprojekter.
K: Jamen det var nogle penge jeg havde investeret, og for at jeg kunne få dem udbetalt. Det var de her banker de samarbejder med. Nej nej sagde hun (red. svindleren). Det er heller ikke lån, de kan overføre de der penge til mig. Implicit har jeg forstået at de penge der var på den der Bitcoin konto, altså det blev betalt til det her lånefirma, der overførte pengene til mig. ..."

Den 19. februar 2023 gjorde klageren indsigelse overfor sparekassen og anførte:

"Som I ved, har jeg desværre været udsat for phising/datasvindel, idet for mig ukendte personer, vha social engineering har skaffet sig adgang til min bankkonto og franarret mig mange penge ved at udgive sig for, at være et investeringsfirma Det viste sig desværre at være ulov1ig phising/datasvindel.

Jeg har talt med en advokat hos retshjælpen om min retsstilling, da jeg naturligvis er ked af, at jeg har ladet mig snyde og er franarret mine penge. Jeg vil derfor gerne gøre opmærksom på, at banken som udgangspunkt skal tilbagebetale de penge der er hævet på min konto og at jeg sandsynligvis har en selvrisiko på optil 8000 kr., da jeg har ladet mig snyde og godkende adgang til min bankkonto...."

Klageren medde1te, at hun gjorde indsigelse overfor følgende transaktioner:

"…
Opsparingskonto:
13.12 er der hævet 45.000 kr. og 5.1 er der tilbageført 36.253.54 kr. fra Danske bank
23.12 er der hævet 2 x 10.000 kr.
23.12 er der returneret 21.000 kr. fra ???
23.12 er der lavet to straks overførsler fra kontoen på 46.000 kr +1.000 kr
23.12 går der 50.000 kr. ind fra [P1]. (Penge lånt i mit navn)
19.12 hæves der 50.000 kr.
16.12 indsættes der 50.000 kr. fra ??'?
Posteringer fra madkontoen
28.12 x 2 450 EUR til [B], Vilnius.
…"

Af en fremlagt kontoudskrift fremgår to kortbetalinger på henholdsvis 450 EUR og 100 EUR den 28. december 2022. Sparekassen har fremlagt en oversigt over SMS'er sendt til klagerens telefonnummer, blandt andet med oplysning om koder til køb hos to kryptovalutabørser, B og C på 450 EUR og IOO EUR den 23. december 2022 samt udskrift fra sit system vedrørende kortbetalingen til B, hvoraf det fremgik, at betalingen var indløst med sikkerhedsløsningen 3 D Secure.

Sparekassen har fremlagt en oversigt over IP-adresser brugt via klagerens netbank i perioden fra den 13. til den 24. december 2022.

Sparekassen har endvidere fremlagt korrespondance med sparekassens datacentral, som forestår udsendelse af SMS'er på vegne af sparekassen, hvoraf det blandt andet fremgår:

"…

l forhold til transaktionen på 45.000 d. 13/12 2022, så kan jeg desværre ikke levere en log der præcist beviser, at der er sendt en SMS til ... om det. Det jeg kan gøre er flg.: Sessionsloggen viser, at transaktionen på de 45.000 er foretaget i en netbank session der starter 13/12 2022 kl. 10:18. Transaktionen er foretaget fra den samme computer/browser som er blevet brugt i alt "165 gange siden d. 30/3 2022 og 25/6 2022. Det er således overordentlig sandsynligt, at det er kundens egen stationære/bærbare Windows 7 PC. Så vi ved, at transaktionen er udført fra kundens egen pc. For at transaktionen kunne blive gennemført, så blev der krævet en engangskode. Denne engangskode er blevet indtastet korrekt. Så hvis det ikke er kunden selv, så er engangskoden alligevel blevet indtastet på kundens egen pc. Hvordan har en eventuel svindler som angiveligt skulle have modtaget denne SMS kunne indtaste den på kundens egen PC? Ikke alene er transaktionen udført fra kundens egen PC. Der er også anvendt den samme IP-adresse som kunden har brugt i månedsvis. Så kundens egen PC har stået samme sted hvor den plejer.

…"

Ankenævnet traf afgørelse om, at nævnet ikke kunne behandle sagen.

I begrundelsen siges det bl.a.:

"…
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 svigagtigt, eller at betaleren har undladt at opfylde sine forpigte1ser, jf. betalingslovens § 93.

Ankenævnet finder, at klagerens MitlD var en personlig sikkerhedsforanstaltning, jf. betalingsloven § 7, nr. 31. Ved transaktionerne blev der anvendt stærk kundeautentifikation, jf. betalingsloven § 7, nr. 30.

Ankenævnet finder, at en afklaring af de nærmere omstændigheder, herunder om transaktionerne skete under omstændigheder, der medfører, at klageren hæfter fuldt ud eller delvist efter betalingslovens § 100, stk. 4 eller stk. 5, forudsætter en yderligere bevisførelse i form af parts- og vidneforklaringer, der ikke kan ske for Ankenævnet, men som i givet fald må finde sted for domstolene.

…"

Af betydning er bl.a. fremlagt en WhatsApp korrespondance mellem S1 og en ukendt person, benævnt Jane, af S1 betegnet som "svindle-ren". Af korrespondancen, der foregik i perioden 14. december 2022 til den 27.

januar 2023 fremgår, at S1 den 15. december 2022 forlanger at få tilba-gebetalt nogle penge og den 16. december 2022 angiver, at hun ønsker de 45.000 kr. tilbagebetalt, som personen stjal fra hende.

"A" har som fagkyndig ansat ved Sparekassernes Data Cen-tral SDC på baggrund af en række spørgsmål fra sagsøgte i mail af 21. februar 2025 udtalt sig bl.a. som nedenfor anført:

> "…
>
> Fortæl lidt om din baggrund og dine arbejdsopgaver i SDC.
> *Jeg har arbejdet i SDC siden 1996. Siden 2015 har jeg arbejdet med vores Anti-fraud system. Arbejdet indebærer bl.a. opbygning af regler/scenarier, behandling af henvendelser fra banker, udarbejdelse af bevismateriale til efterforskning, levering af logfiler m.m.*
>
> Kan du overordnet forklare hvilke sikkerhedstiltag der er forbundet med selvbetjeningsløsningen Netbank i Sparekassen Balling.
> *Helt overordnet: Der kræves MitID for at logge ind i netbanken, og der kræves ligeledes MitID når en transaktion skal signeres. Herudover kan nogle transaktioner endvidere kræve en engangskode som udsendes i en SMS til det mobilnummer som forinden er registreret på kunden.*
>
> Kan du forklare hvordan en straksoverførsel i Sparekassen Balling finder sted og hvad fremgangsmåden er for at en overførsel kan gennemføres pr. december 2022?
> *En straksoverførsel gennemføres på samme måde som jeg har anført ovenfor. Selve proceduren for en straksoverførsel afviger ikke markant fra andre type, bortset fra, at Sparekassen typisk har sat andre grænser for hvornår en SMS-kode skal kræves. Typisk kræves en SMS-kode ved et lavere beløb på en straksoverførsel end det er tilfældet ved en almindelig dag-til-dag overførsel.*
>
> Hvor stor skal en overførsel være, pr december 2022, før man får en sms med et one time password (OTP)?
> *Det ved jeg ikke. De enkelte banker bestemmer selv deres beløbsgrænser ved de forskellige typer overførsler, og disse kan ændres løbende. Jeg har ikke et register over hvordan Sparekassen Ballings grænser var på en bestemt dato.*
>
> Sagsøger nægter at have modtaget de 3 OTP-koder for nedenstående udgående straksoverførsler fra sagsøgers konti. Hvad er din vurdering af det?
> • konto 1 kr. 45.000 d. 13-12-2022.
> *Sessionsloggen viser, at transaktionen på de 45.000 DKK er foretaget i en netbank session der starter 13/12 2022 kl. 10:18.*
> *Transaktionen er foretaget fra den samme computer/browser som er blevet brugt i alt 165 gange siden d. 30/3 2022 og 25/6 2022. Det er således overordentlig sandsynligt, at det er kundens egen stationære/bærbare Windows 7 PC.*

Så vi ved, at transaktionen er udført fra kundens egen pc. For at transaktionen kunne blive gennemført, så blev der krævet en engangskode. Denne engangskode er blevet indtastet korrekt.

• konto 2 hhv. 50.000 kr. d. 19-12-2022 og 46.000 kr. d. 23-12-2022. *Vores SMS-log fra d. 23/12 2022 viser, at de er sendt en SMS med en engangskode på transaktionen på de 46.000. Den er sendt d. 23/12 kl. 12:22. SMS-loggen viser, at SDC's leverandør SMS-leverandør Sinch har afleveret SMS'en til sagsøgers operatør/udbyder kl. 12.22.*

Sparekassens egne udskrifter og kundens kontoudtog viser, at denne transaktion er blevet bogført. Derfor er engangskoden blevet indtastet korrekt. Ellers kunne transaktionen ikke gennemføres.

Transaktionen på de 50.000 DKK kan vi ikke direkte bevise at der er udsendt SMS på, men forklaringen er den samme som den på 45.000 DKK:

Den er beviseligt udført fra den samme PC som er brugt 165 gange siden 30/3. Den er udført fra samme pc hvorfra der også bl.a. er betalt et girokort på 200 DKK d. 22/11. Så vidt jeg ved, er der ikke gjort indsigelse med denne transaktion, hvorfor det med meget stor sandsynlighed er kundens egen PC.

Hvad fortæller hhv. Bilag L og M?
Bilag L er en SMS-log fra SDC's SMS-leverandør Sinch. Den viser de SMS'er er der sendt til kunden i et tidsinterval. De fremhævede linier i bilaget viser (med rødt) en information til kunden om at der er brugt et kort til køb hos "Binance" på 450 EUR.
Med gult vises at der er sendt en SMS til kunden med en engangskode i relation til gennemførslen af en transaktion på 46.000 DKK.
Bilag M viser et skærmbillede fra SDC's anti-fraud system. Det er et system der overvåger, logger og alarmer på netbank transaktioner. Billedet viser en transaktion på 45.000 DKK som er signeret d. 13/12 2022 kl. 10:23:54. Den viser endvidere at transaktionen er foretaget i Sparekassen Ballings netbank, og at den er gennemført ved indtastning af en 6-cifret SMS-kode XXXXXX". Denne SMS-kode kan KUN komme fra en SMS som er sendt til kunden, og dens korrekte indtastning er en forudsætning for at transaktionen kan sig-neres.
SMS-koden er indtastet korrekt kl. 10:23:25

På hvilken enhed mener du de 3 OTP-koder er indtastet for så vidt angår de ovennævnte transaktioner, og af hvem?
På baggrund af de ovennævnte forhold og de i bilag K beskrevne forhold, er det min vurdering at de tre SMS'er er indtastet på sagsøgers egen PC.
Den PC som er blevet brugt i tiden op til de bestridte transaktioner.

Hvis det forudsættes (jf. vedhæftede bilag 3) at der har været anvendt Any

Desk, hvilken betydning har det haft for overførslerne?
Vi har ingen mulighed for at se hvorvidt nogle af transaktionerne er udført via Anydesk. På daværende tidspunkt efterlod brugen af Anydesk ikke nogen spor i vores systemer. Vi kan alene se, at de er udført fra sagsøgers pc.

"A" er videre stillet en række spørgsmål angående anvendel-sen af værktøjet Anydesk. Af udtalelsen, der er dateret 20. marts 2025 fremgår:

"…
1. Er du bekendt med Anydesk? Hvis ja, beskriv gerne, hvad det er og kan?
Ja. Det er et program til fjernstyring af f.eks. en PC, Mac eller mobiltelefon. Det skal manuelt installeres på den enhed man ønsker skal fjernstyres.
Herefter kan den som fjernstyrer benytte sin egen mus, tastatur, skærm m.v. til at udføre handlinger på den fjernstyrede pc, ligesom hvis man selv sad fysisk ved pc'en.

2. Er det efter din opfattelse teknisk muligt at nogle af transaktionerne i sagen er udført/gennemført via eller eventuel med hjælp fra Any-Desk? Det bedes tillige oplyst, hvilken betydning det kan have?
Det er teknisk muligt at nogle af transaktionerne i sagen er udført på en måde, hvor Anydesk er benyttet.
Det kan have haft den betydning, at sagsøger ikke selv fysisk har betjent mus eller tastatur i forbindelse med gennemførslen af transaktionerne.

3. I bekræftende fald ønskes det oplyst, hvorvidt brugen af Anydesk vil kunne påvises?
Det er ikke muligt for SDC eller Sparekassen Balling at påvise om der er brugt Anydesk. Anydesk er et program som installeres på brugerens PC. Vi overvåger ikke hvad brugeren har valgt at installere på sin PC.

4. Det ønskes uddybet hvad du i dit svar mener med, at " brugen af Anydesk ikke efterlader spor i jeres system"
I vores system har vi ikke nogen logning der viser, at det er brugeren selv der fysisk har trykket på tastaturet eller har bevæget musen, eller om disse input er kommet ind via Anydesk. Vi registrerer hvilke funktioner der bliver anvendt og hvilket indhold der er i de forskellige felter og skærmbillede.
Det skal understreges, at Anydesk ikke af sig selv kan blive installeret på en PC. Hvis det har været i brug i denne sag, så har sagsøgte (eller anden med fysisk adgang til PC'en) manuelt valgt at installere programmet.
Endvidere kræves der en Anydesk adresse for at kunne fjernstyre en PC via Anydesk. Denne adresse vises når man starter Anydesk på sin PC. Denne adresse skal formidles til personen der ønsker at fjernstyre.
Først herefter vil det være muligt at fjernstyre PC'en via Anydesk.
Ved normal brug af Anydesk vil flytning af mus og indtastning via tastatur være synligt på kundens skærm, således at man vil kunne se at der er aktivitet på skærmen.
…"

Sagsøgte har yderligere fremlagt følgende transskription af telefonsamtale mel-lem sagsøger og kundemedarbejder (MM), Sparekassen Balling, den 13. december 2022 kl 09:46, varighed 55 sekunder.

"…
MM: Sparekassen Balling, det er MM
Sagsøger: Hej MM jeg tror måske "B" (red: medarbejder i Sparekas-sen) har forsøgt at ringe til mig. S1.
MM: Nej, det er mig. Det er fordi dit kort er blevet spærret af Nets, fordi der er to posteringer der dog er blevet afvist, fordi man er i tvivl om det er dig, på 7.500 kr. I går aftes kl 18:55.
MM: Det er dig selv der har afvist dem?
Sagsøger: Ja, det er det
MM: Det er noget der hedder MoonPay.
Sagsøger: Ja, det er korrekt.
MM: Men det er dig selv der afviser, okay.
MM: Godt, så åbner jeg dit kort igen, så kan du kan komme videre med julehand-len.
…"

Forklaringer

S1 har forklaret, at hun bor i et andelsboligfællesskab i x-by. Hun modtager som følge af en hjerneblødning opstået under et ophold i X-land i 2017 førtidspension. Hun har problemer med overblik, initiativ og forestillings-evne og bliver let presset. Hun er dårlig til klar/parat spørgsmål.

Sagen startede med, at hun i december 2022 blev kontaktet af en person, Jane, fra firmaet Binance. Jane talte engelsk. Jane fortalte, at hun var sat til at lukke sagsøgerens bitcoininvesteringskonto ned. Det lød overbevisende, da sagsøge-ren en gang havde investeret i bitcoin. Det blev sagt, at det var et ikke ubetyde-ligt beløb, der stod på kontoen. 20.000 euro blev nævnt. Jane fik procenter i kommission for at hjælpe. For sagsøgeren lød det fantastisk, og hun tænkte på, at hun endelig havde noget medvind.

Under en telefonsamtale ville Jane installere et program på sagsøgerens PC, så kunne hun hjælpe med pengeoverførslen. Jane sendte et link, som sagsøgeren trykkede på. Det var programmet Any Desk, der nu blev installeret, og så hav-de Jane adgang til sagsøgerens PC, når blot sagsøgeren "lukkede hende ind". Efter installeringen ringede Jane hver formiddag og fik sagsøgeren til med sit NemID at logge på sin netbank, idet Jane ellers ikke kunne komme ind.

I starten blev der ikke overført penge, det var først lige før Jul, da hun ville købe gaver til sit barnebarn, at hun opdagede, at hendes konti alle var tømte.

Sagsøgeren har ikke selv gjort noget. Det var svindleren, der styrede det hele, så snart denne var kommet ind på hendes netbank. Sagsøgeren gav aldrig svindleren sit MitID, men hun loggede på, når svindleren bad hende om det.

Hun husker intet til den samtale, det siges, at hun havde med sparekassemedar-bejderen den 13. december 2022. Hun husker heller ikke, at hun skulle have spærret sit kort. Hun husker ikke, hvornår hun første gang snak-kede med nogen fra sparekassen.

Det er hende uforståeligt, at sparekassen ikke har reageret. De er sat i verden for at passe på hendes penge. De småbeløb, der er hævet den 12. og 13. december er det sandsynligvis hende selv, der har hævet. Tilsvarende gælder 2.000 kr. den 19. december til "madkonto". Hævningerne i dollars siger hende intet.

Hun har aldrig fået nogen sms-er fra sparekassen, og hun har ikke godkendt nogen overførsler. Hun opdagede først, at der var sket svindel, da hun fandt ud af, at hendes konti var tømt. Da Jane ringede, foreholdt hun Jane, at pengene var væk. Jane svarede, at det var ubetydelige beløb. Hun fik også på et tidspunkt at vide, at de havde taget et "depositum", og at det var fordi det ikke skulle se ud som hvidvask.

Hun kan ikke svare på, hvorledes det kan gå til, at der er indlæst sms-koder til hævning, når hun ikke har modtaget sms-erne. Svindlerne har aldrig haft kontrol over hendes telefon eller hendes MitID. Hun har afvist at fremlægge logudskrifter fra sin telefon, der kunne be -eller afkræfte, at hun har modtaget sms-er. Hun kan ikke svare på, hvorfor hun ikke har villet fremlægge loggene.

Hun kan bekræfte, at der er optaget lån i flere banker i hendes navn, bl.a. Bank of Egypt. Jane sagde, at det var nogle banker, de samarbejdede med. De banker, der gav hende lån, så ingen form for dokumentation fra hende, hverken indkomstoplysninger, skatteoplysninger eller andet.

Hun har været i fogedretten med Express Bank, de truede med bål og brand. Hun sagde, at det var svindel det hele, og at hun intet ejede.

Hun kontaktede ikke banken, da hun opdagede, at hun var svindlet, fordi hun følte sig flov over at være hoppet i sådan en fælde. Hun har siden politianmeldt det. Politiet siger, at sagen indgår i et større hvidvaskkompleks, der har relation til Nordjyllands Politi.

Der er også en fra Løgstør, der har taget penge fra hendes konto.

Foreholdt, at hun allerede i samtale den 16. december har foreholdt svindlerne, at de havde stjålet fra hende, må hun erkende, at så har hun vidst dette allerede på det tidspunkt.

Parternes synspunkter
S1 har i sit påstandsdokument anført:

> "…
> Det gøres gældende, at betingelserne i betalingslovens § 100, stk. 3. er opfyldt, idet sagsøger har været udsat for tredjemands misbrug af hendes betalingstjeneste og at personlige sikkerhedsforanstaltninger har været anvendt.
>
> Misbruget består i, at sagsøger under diverse telefonsamtaler er blevet manipuleret og snydt af "svindleren", herunder idet denne pressede sagsøger til at installere et fjernstyringsprogram, Anydesk, på hendes PC og telefon, hvor overførslerne er foretaget af andre end sagsøger.
>
> Sagsøger, der har en hjerneskade som følge af hjerneblødning, blev meget presset af "svindlerens" henvendelser, og sagsøger skal som forbruger i denne sammenhæng beskyttes og kompenseres mod professionel og organiseret svindel, hvilket da også er udgangspunktet i betalingslovens § 100.
>
> Sagsøger har herefter krav på tilbagebetaling, svarende til det påstævnte beløb.
>
> Det bestrides, at sagsøger skulle have handlet forsætligt, svigagtig eller uagtsomt, ligesom det bestrides, at betalingslovens § 100, stk. 5 finder anvendelse.
>
> Til støtte for den subsidiære påstand gøres det gældende, at forholdene som minimum er omfattet af betalingslovens § 100, stk. 4., hvorefter sagsøger hæfter for en selvrisiko på kr. 8.000, hvorefter den subsidiære påstand udgør kr. 162.000 fratrukket selvrisiko kr. 8.000, således i alt kr. 154.000.
>
> Ved vurderingen af om et forhold er omfattet af betalingslovens § 100, stk. 4 lægges der vægt på, om betaler (sagsøger) har følt sig presset jf. bl.a. afgørelsen 221/2021 ved det finansielle ankenævn.
>
> Det gøres gældende, at sagsfremstillingen vidner om, at sagsøger utvivlsomt har følt sig presset. …
>
> Herudover lægges der vægt på, om forholdet kan karakteriseres som phising. Det gøres gældende, at forholdene i sagen udgør phising, da sagsøger er blevet lokket til at give svindlerne fortrolige oplysninger.

Det gøres gældende, at selvom, at transaktionerne er korrekt registeret og bogført og ikke ramt af tekniske svigt eller andre fejl, er det ikke ensbetydende med, at sagsøger har godkendt transaktionerne jf. betalingslovens § 98, stk. 2.

Slutteligt bestrides det, at betalingslovens § 100, stk. 5 finder anvendelse, idet bestemmelsen alene finder anvendelse såfremt betalerens udbyder godtgør, at betaler med fortsæt til, at der skulle foretages den uberettigede anvendelse, har oplyst sine personlige sikkerhedsforanstaltninger. Det er sagsøgte, der har bevisbyrden for dette, og denne bevisbyrde har sagsøgte ikke løftet.

…"

BALLING SPAREKASSE har i sit påstandsdokument anført:

"…
Til støtte for frifindelsespåstanden gøres det gældende

- Vedr. transaktionen kortbetaling 450 EUR til "Binance
At betalingen er gennemført med 3D-secure, hvilket vil sige, at sagsøger godkendte betalingen i mitID-app ved at "swipe", og dermed illustrerede sin risikovillighed til at betale penge for at realisere den påståede gevinst.

At sagsøger ikke har dokumenteret, at hendes kontooprettelser i "Binance" har påført sagsøger et tab.

- **Vedr. transaktionerne på 45.000, 46.000 og 50.000 kr.**
At sagsøger – ud fra det oplyste – ikke blev opfordret, presset eller bedraget til at udlevere sine personlige sikkerhedsforanstaltninger, betalingslovens § 7, nr. 31) dvs.
1. MitID bruger-ID
2. Pinkode til MitID app eller nøgleviser
3. adgangskode til mobiltelefon, enten kodeord, fingeraftryk eller ansigtsgenkendelse, og
4. engangskoderne, der blev fremsendt via SMS til mobiltelefon

At sagsøger ikke udviste den fornødne agtpågivenhed og overvejede ægtheden, da en engelsktalende svindler henvendte sig uopfordret, og at dette skete under omstændigheder hvor sagsøgeren indså eller burde have indset, at der var risiko for misbrug.

At gennemgangen i bilagene D og 3 af sagsøgers omgang med svindlerne illustrerer sagsøgers adfærd og risikovillighed ved ønske om investering af Bitcoins, samt udtalelsen umiddelbart efter kontakten ophører med

svindlerne "*Dumhed, tror jeg. Det er dyrt at være fattig, så falder man for alt muligt mærkeligt*" viser sagsøgers anger.

at det for svindlerne ikke er muligt at skaffe sig adgang til nr. 1-4 jf. ovenfor – uden sagsøgers mellemkomst - og dermed sagsøgers netbank og foretage overførslerne, uden at sagsøger selv – bevidst eller ubevidst – medvirkede hertil.

at sagsøger ikke har kunnet sandsynliggøre, at uvedkommende tredjemænd – uden sagsøgers mellemkomst- via hacking eller overtagelse af E-simkort skaffede sig adgang nr. 1-4 jfr. ovenfor herunder adgang til OTP-sms'erne.

at den påståede adgang via. "Anydesk" fjernstyring ikke underbygger, at uvedkommende skulle have skaffet sig adgang til alle elementer af sagsøgerens personlige sikkerhedsforanstaltninger.

At sagsøger var i kontakt med svindlerne i hvertfald den 13. december 2022 og formentlig tidligere end denne dato, hvor sagsøgers kort blev spærret grundet 2 betalinger til "MoonPay", men at sagsøger vedkendte betalingerne selv om disse ikke gik igennem og valgte at bede om genoplåsning af sit kort og foresatte sit forehavende og dermed afkræftede mistanken overfor Sparekassen.

At sagsøger modtog samtlige OTP-sms'er i kombination med at disse blev indtastet af sagsøger på samme PC og af samme IP-adresse som anvendt 165 gange tidligere siden 30.03.2022 og 25.06.2022

At sagsøger var i stand til at betjene og havde fuld kontrol over sine selvbetjeningsløsninger i Sparekassen Balling før, under og efter svindlen, grundet de vedkendte betalinger før og efter hændelserne, hvilket ikke ville være tilfældet, hvis svindlerne havde lavet et komplet identitetstyveri og havde overtaget sagsøgerens MitID.

At svindlerne ikke kunne have indtastet sms-koderne via "Anydesk".

Det må have formodningen imod sig at sagsøger aflæser sms-koderne for så at videregive denne til svindlerne, men derimod har indtastet disse selv.

At sagsøgers undladelse af at gøre indsigelser i dagene 13. december 2022 til 22. december 2022 eller efter seneste kontakt med svindlerne underbygger at sagsøger selv autoriserede og foretog transaktionerne, men snarere fortrød sine betalinger for at få bitcoins "ud" og i strid med

det faktisk passerede at transaktionerne ikke var udtryk for andres uberettigede anvendelse af hendes personlige sikkerhedsforanstaltninger.

At det sammenfattende er ubetænkeligt at lægge til grund, at sagsøger selv autoriserede transaktionerne jf. lov om betalingers § 82, stk. 1, idet sagsøger selv initierede og gennemførte de omhandlende overførsler og at forholdet derfor falder uden for lovens § 100.

Ved vurderingen af om et forhold falder udenfor loven, bør man skele til den seneste praksis af 3. maj 2023, der er vedlagt som bilag, hvor Københavns Byret (sagsnr. BS-15629/2022-KBH) frifandt Lån og Spar Bank et pengeinstitut der anvender SDC-systemer som Sparekassen Balling. Sagen, der er meget lignende nærværende sag, omhandlede en kvinde der blev kontaktet af en engelsktalende mand, som tilbød at hun kunne købe bitcoins hvilket endte med 3 overførsler, der senere blev gjort gældende var uautoriserede betalinger. Retten lagde til grund at sagsøgerens personlige sikkerhedsforanstaltninger var blevet anvendt, og fandt det bevist at SMS-koderne var blevet leveret og indtastet af netop sagsøgeren på baggrund af tekniske logs og vidneforklaringer fra medarbejdere hos datacentralen SDC A/S.

At sagsøger fortsætter med at være i dialog med svindlerne i januar 2023 og dermed accepterer risikoen for yderligere svig, selv om man er i dialog med Sparekassens medarbejdere, der forsøger at redde det tabte.

- Vedr. alle betalinger
At samtlige omtvistede betalinger er sket med stærk kundeautentifikation jf. lov om betalinger § 7, nr. 30, hvor autentifikationen er baseret på anvendelsen af to eller flere elementer, der er kategoriseret som viden, besiddelse og iboende egenskab, der er uafhængige, så brud på et element ikke svækker pålideligheden af de andre elementer, og er designet på en sådan måde, at fortroligheden af autentifikationsdata beskyttes.

- Vedr. optagelse af lånene som blev udbetalt til sagsøgers konto i Sparekassen
At sagsøger ikke har forsøgt at tabsbegrænse ved indgive falskindsigelse til de långivende pengeinstitutter.
At det må have formodningen imod sig, at svindlerne kan ansøge to pengeinstitutter om, og der kan bevilliges to lån, uden videre og uden sikkerhedsstillelse fra sagsøger, uden der har været en udførlig kreditvurdering af sagsøgers økonomiske forhold uden sagsøgers medvirken hertil, hvilket også fremgår af beskeden fra sagsøger til svindleren den 20.12.2022 kl 22.14.

At lovens ånd i lov om betalinger sammenholdt med European Banking Authoritys (EBA) guidelines ikke taler for den urimelige situation, at ét pengeinstitut, nemlig Sparekassen, vil skulle dække tabet både for sag søgeren, men også for de andre involverede pengeinstitutter, blot fordi lånene formentlig udbetales til klagerens Nemkonto i Sparekassen. Sag-søgerens lån hos andre institutter og eventuelle ugyldighedsspørgsmål herom vedkommer i denne sammenhæng ikke sagsøgte.

- Vedr. sagsøgers helbredsoplysninger
at sagsøgte på intet tidspunkt omkring det passerede havde viden om, at sagsøgte ikke var i stand til at handle fornuftsmæssigt.
…"

Rettens begrundelse og resultat
Det lægges til grund, at S1 er blevet overtalt til at lade en ukendt en-gelsktalende person overtage kontrollen med sin PC via systemet Anydesk, og at S1 desuden har givet vedkommende adgang til sin netbank, og at den ukendte person som følge af foretagne transaktioner har fået overført 162.000 kr.

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 svigagtigt, eller at betaleren har undladt at opfylde sine forpigte1ser, jf. betalingslovens § 93.

Det anses utvivlsomt, at S1s MitlD var en personlig sikkerhedsforan-staltning, jf. betalingsloven § 7, nr. 31.

Ved de omhandlede transaktioner blev der efter det for retten oplyste anvendt stærk kundeautentifikation, jf. betalingsloven § 7, nr. 30.

Det er S1s påstand, at hun ikke har videregivet oplysninger angående sit MitID til svindlerne, lige som det er hendes påstand, at Sparekassen ikke har sendt sms-koder til hende.

Ved den fremlagte dokumentation i form af udtalelserne fra "A" er der skabt et høj grad af formodning for, at der er afsendt sms-er og at der derfor til de tre store hævninger er anvendt sagsøgerens telefon, eller at S1 har videregivet oplysninger fra telefonen relaterende til sit MitID.

Idet S1 har oplyst, at hun på alle tidspunkter har haft fuld rådighed over sin telefon, er formodningen derfor for, at hun selv har benyttet sin telefon til at godkende de tre største hævninger og derved aktivt medvirket til, at svindlerne kunne hæve de omhandlede beløb.

S1 har haft mulighed for at afkræfte denne formodning, idet hun er opfordret til at fremlægge fuldstændige logoplysninger for sin telefon, men det har hun ikke villet.

Retten lægger derfor til grund, at S1 har benyttet sin telefon til at medvirke til, at svindlerne kunne hæve de omhandlede beløb.

Under hensyn til, at den person, der havde kontaktet S1 var uden-landsk og ganske ukendt for S1, finder retten, at S1 ved at hjælpe personen til at hæve de omhandlede beløb, har handlet groft uforsvar-ligt, jf. herved betalingskortlovens § 100, stk. 3, nr. 2 og nr. 3. Efter disse bestem-melser har S1 krav på at få dækket sit tab, fradraget selvrisikoen på 8.000 kr.

Som det fremgår af den fremlagte transkription af S1s korrespon-dance med svindleren, gav S1 den 16. december 2022 udtryk for, at personen havde stjålet 45.000 kr. fra hende.

Retten lægger derfor til grund, at S1, da hun godkendte hævningerne den 19. og den 23. december 2022 og skaffede svindleren adgang til at foretage de øvrige hævninger i samme tidsrum, positivt vidste, at der var en nærlig-gende risiko for misbrug.

Retten finder derfor, at alle disse senere betalinger er omfattet af betalingskort-lovens § 100, stk. 5, og at S1 derfor selv hæfter for det tab, hun herved har lidt.

Retten tager herefter S1s påstand til følge med 45.000 kr., hvor fradrages selvrisikoen på 8.000 kr., således at det endelige beløb udgør 37.000 kr.

Efter sagens udfald ophæver retten sagens omkostninger.

THI KENDES FOR RET:

Sagsøgte, Balling Sparekasse, skal inden 14 dage til sagsøgeren, S1, be-tale 37.000 kr. med tillæg af procesrente fra den 2. juli 2024.

Ingen af parterne betaler omkostninger til den anden part.

Vejledning

Retten har afsagt dom i sagen.

Hvis du er utilfreds med afgørelsen, kan du som udgangspunkt anke (klage over) dommen til landsretten. Hvis du kun er utilfreds med dommens afgørelse om sagsomkostninger, kan du kære (klage over) denne del af afgørelsen til landsretten.

Ikke alle afgørelser kan ankes eller kæres
Du kan kun anke dommen, hvis forskellen mellem byrettens dom og det resultat, du ønsker at opnå i landsretten, er over 50.000 kr. Hvis forskellen er mindre, skal du have tilladelse fra Procesbevillingsnævnet for at anke.

Landsretten kan afvise at behandle en ankesag, hvis landsretten vurderer, at der ikke er udsigt til, at sagen vil få et andet udfald i landsretten.

Du kan kun kære afgørelser om sagsomkostninger, hvis omkostningsbeløbet er fastsat til mere end 50.000 kr., eller hvis retten har bestemt, at ingen af parterne skal betale sagsomkostninger, og du kræver, at modparten skal betale mere end 50.000 kr. I andre situationer kan du kun kære omkostningsafgørelsen, hvis du får tilladelse fra Procesbevillingsnævnet.

Frister for at anke og kære
Fristen for at anke er **4 uger** fra dommens dato. Hvis du ikke kan anke uden en tilladelse fra Procesbevillingsnævnet, skal du indlevere en ansøgning til Procesbevillingsnævnet inden **4 uger**.

Fristen for at kære omkostningsafgørelsen er **2 uger** fra dommens dato. Hvis du ikke kan kære afgørelsen uden tilladelse fra Procesbevillingsnævnet, skal du indlevere en ansøgning til Procesbevillingsnævnet inden **2 uger** fra dommens dato.

Sådan gør du, hvis du vil anke eller kære

Du kan anke dommen på minretssag.dk ved at trykke på knappen "Opret appel" og derefter vælge "Anke" og følge vejledningen. Hvis du vil kære omkostningsafgørelsen, skal du vælge "Kære" og følge vejledningen.

Du kan læse mere på domstol.dk.

Hvis du ønsker at søge om tilladelse til anke eller kære, skal du indlevere en ansøgning til Procesbevillingsnævnet på www.procesbevillingsnaevnet.dk eller mail til post@procesbevillingsnaevnet.dk eller post@pbn.dk. Procesbevillingsnævnet har adresse på Store Kongensgade 1, 2. sal, 1264 København K. Du kan ikke indlevere ansøgningen på minretssag.dk.