RETTEN I VIBORG
DOM

afsagt den 23. juni 2023

Sag BS-34279/2020-VIB

Sagsøger
(advokat Torben Jensen)

mod

Jyske Bank A/S
(advokat Erik Bertelsen)

Denne afgørelse er truffet af Dommer 1, Dommer 2 og Dommer 3.

Sagens baggrund og parternes påstande
Sagen, der er anlagt den 3. september 2020, drejer sig om, hvorvidt Jyske Bank A/S hæfter for to overførsler på 446.299,36 kr. fra en kundes konto til en uden-landsk virksomhed, herunder om der er tale om uautoriserede overførsler.

Sagsøger har nedlagt følgende påstand:

Principalt
Jyske Bank A/S skal til Sagsøger betale 446.299,36 kr. med procesrente fra den 7. marts 2018.

Subsidiært
Jyske Bank A/S skal til Sagsøger betale 445.924,36 kr.

Mere subsidiært

Jyske Bank A/S skal til Sagsøger betale 438.299,36 kr. med procesrente fra den 7. marts 2018.

Sagsøgte, Jyske Bank A/S, har nedlagt påstand om frifindelse, subsidiært betaling af et mindre beløb.

Oplysningerne i sagen

Sagsøger havde i 2017 og 2018 to konti i Jyske Bank A/S. Der blev fra den ene konto den 6. marts 2018 overført henholdsvis 9.800 euro og 50.000 euro, eller i alt 446.299,36 kr., til EVG Trading Limited. Sagsøger påstår, at Jyske Bank A/S hæfter for hendes tab i forbindelse med disse over-førsler.

Det fremgår af kontoudtog vedrørende kontiene, at der i perioden fra den 3. de-cember 2017 og frem til ovennævnte overførsler blev overført i alt 237.777,39 kr. ad 11 gange fra kontiene til Greenfields Capital eller andre investeringsselska-ber med tilknytning hertil, herunder EVG Trading Limited. Der blev herunder den 6. marts 2018 henholdsvis kl. 15.59.10 og kl. 16.00.22, kort før de omtvistede overførsler, overført 1.000 euro eller 7.562,55 kr. Der blev i samme periode ud-betalt 25.681,65 kr. ad 6 gange fra Greenfields Capital til kontiene. Den 7. marts 2018 henstod der 73.139,36 kr. på den konto, hvorfra de sidste to overførsler skete.

Af log detaljer vedrørende ovennævnte overførsler fra Sagsøgers konti fremgår det, at der ved overførslerne foretaget den 8. og 18. januar 2018 og 28. februar 2018 blev brugt en computer med samme styresystem og samme browser som ved de to omtvistede overførsler den 6. marts 2018. Der blev end-videre benyttet den samme IP-adresse ved overførslerne den 8. og 18. januar 2018 og den 6. marts 2018. De to overførsler på hver 1.000 euro den 6. marts 2018 blev foretaget fra samme IP-adresse og med de samme oplysninger om an-vendt styresystem, browser, teleselskab og geografisk lokation i Danmark, som de to omtvistede overførsler.

Der fremgår videre af log detaljerne, at der ved overførslerne den 6. marts 2018 blev brugt 2-faktor godkendelse ved den første overførsel kl. 16.23.31, og at der blev brugt 1-faktor godkendelse ved den anden overførsel kl. 16.30.05.

Der er fremlagt mailkorrespondance mellem Sagsøger og Green-fields Capital for perioden fra den 7. december 2017 til den 28. marts 2018.

Af mailkorrespondancen fremgår det bl.a., at Sagsøger den 7. og 8. december 2017 skrev om investering i bitcoins med Greenfields Capital. Den 5. februar 2018 modtog Sagsøger efter forespørgsel herom betin-gelserne for at hæve beløb fra sin konto hos Greenfields Capital. Den 9. marts 2018 kl. 19.20 skrev Sagsøger, at hun ikke troede på Greenfields Capital, når de oplyste hende om, at de ikke kunne få kontakt til hendes seneste sagsbehandler. Kl. 19.47.04 skrev Sagsøger, at hun havde prøvet at overføre 4.000 euro, men at der var blevet overført 62.000 euro, og kl. 21.34 meddelte Sagsøger, at hun ønskede at hæve 60.000 euro fra sin konto. Greenfields Capital meddelte ved mail af den 28. marts 2018, at det ikke var muligt at udbetale penge, da der havde været et tab vedrørende kontoen.

Sagsøger kontaktede Jyske Bank A/S den 27. marts 2018. Af en udskrift af Jyske Bank A/S' journalsystem fra den 27. marts 2018 vedrørende Sagsøger fremgår bl.a. følgende:

> *" 27-03-2018: Nemid Spærret. Netbank Spærret, Visadankort spærret. Kunden oplyser, at hun er blevet kontaktet af et Engelsk Bitcoin firma, som hun har indbetalt en del til, både via kort og også som udl. ovf. Hun oplyser, at Firmaet har været med på hendes skærm, og har overfør EUR 50.000 og EUR 9.800 begge den 7/3 i modstrid med aftale om at der skulle overføres 4 x 1.000 DKK. (Dette beløb var en "Forsikring" der skulle bevirke, at hun kunne få det tidligere indbetalte til-bage!) Hun oplyser i øvrigt at have give dem kopi af hendes betalingskort,"*

Sagsøger har afgivet en tro- og loveerklæring, som er underskre-vet den 29. marts 2018, til Jyske Bank A/S. Hun oplyser heri bl.a., at der den 6. marts 2018 uretmæssigt er hævet ca. 10.000 og 50.000 euro på hendes konto. Følgende fremgår af transskriberingen af erklæringen:

" ...

Øvrige oplysninger (fx hvornår og hvordan er transaktionen opdaget og er beløbsmodtager kendt af afsender)

Kontaktet af Green Field Capital Bank ca. ultimo november.
Jeg overførte 1.000 euro. Bankhistorie er kopieret.
Da jeg absolut ikke vil være med mere, bliver jeg tilbudt forsikring, som vil afslutte med at jeg får bonus. Jeg skal overføre 4.000euro og så er alt slut.
Jeg insisterer på at de skal tags fra min Visa konto.
Jeg opdager fredag, at der er taget stort beløb fra hovedkonto.
Jeg har haft Team Wiever (sendt, kendt ?) men sværger på at jeg ikke har set, aftalt eller indvilliget i at overføre beløbet.
Jeg har kopi af min modstand men kan ikke komme ind på min bank.

Jeg har ikke selv på nogen måde foretaget eller accepteret overførslen, hverken via netbank eller på anden måde.

..."

Det fremgår af Jyske Bank A/S' journalsystemet, at Sagsøger den 3. april 2018 blev vejledt om ikke at kommunikere yderligere med Greenfields Capital og om at rense sine enheder. Sagsøger oplyste den 4. april 2018, at hun havde anmeldt sagen til politiet. Den 12. april 2018 meddelte Jyske Bank A/S, at banken afviser godtgørelse, idet det er uklart, om der er tale om uautoriserede overførsler.

Sagsøger klagede til Det finansielle ankenævn, hvis flertal den 18. december 2019 traf afgørelse om, at sagen afvises, idet en stillingtagen til sagen forudsætter en yderligere bevisførelse, som ikke kan ske for ankenævnet.

Forklaringer
Sagsøger, Vidne 1 og Vidne 2 har afgivet forkla-ring.

Sagsøger har forklaret, at hun er pensionist. Hun er uddannet lærer og har arbejdet som skoleleder, herunder med økonomi. Hun er øko-nomisk bevidst og gældfri. Hun er ikke særlig risikovillig i sine investeringer. Hun har været kunde i Jyske Bank i 35 år. Hun og hendes ægtefælle, Person 1, ar-vede ca. 100.000 kr. fra Person 1's far. De ville give beløbet til deres eneste barne-barn på et senere tidspunkt. I mellemtiden ønskede de at investere pengene i en ordning, som de tidligere havde haft hos Jyske Bank, hvor Jyske Bank kunne

handle med værdipapirer for pengene. De kunne ikke miste grundbeløbet, som de havde sat ind på kontoen. De fik halvdelen af overskuddet ved investerin-gen, og den anden halvdel fik Jyske Bank. Jyske Bank havde dog ikke længere denne ordning og ville i øvrigt kræve negativ rente af beløbet, hvis de havde det stående i banken. Hun undersøgte, om der var lignende ordninger hos an-dre banker, men ingen bank kunne tilbyde dem en lignende ordning, medmin-dre de blev hovedkunde hos dem.

Hun kiggede på nettet og fandt en bank ved navn Greenfield Capital, som hun tjekkede på Trustpilot.dk, hvor den fik fine anmeldelser. Hun forsøgte forgæves at ringe til dem. Et kvarter senere blev hun ringet op. Greenfields Capital oply-ste, at hun hos dem kunne få den ordning, hun havde efterspurgt i Jyske Bank, hvis hun investerede minimum 100.000 kr. Hun turde ikke at sende det fulde beløb afsted på én gang, så hun startede med at sende 1.000 euro i december 2017. Hun tænkte ikke dengang nærmere over, at der i korrespondancen med Greenfields Capital var et s på Greenfields. Hun gav Greenfields Capital sine dankortoplysninger. Hun blev efterfølgende nervøs for, om det var okay. Hun spærrede derfor sit dankort og fik tilsendt et nyt. Det var ikke Greenfields Capi-tal som sådan, hun blev nervøs over. Hun blev nervøs for, om hun selv havde gjort noget forkert ved at udlevere sine dankortoplysninger. Det var en del af aftalen med Greenfields Capital, at hun ikke kunne få nogen bonus, inden hun havde indbetalt i alt 100.000 kr. Hun vurderede efterfølgende, at hun godt kunne investere 135.000 kr. Hun overførte beløbene ad flere omgange via kort og netbank. Hun talte hele tiden med nye medarbejdere hos Greenfields Capi-tal. Når hun spurgte efter en af de tidligere medarbejdere, hun havde talt med, kunne de samme dag finde på at sige, at vedkommende både var syg og på fe-rie. Da hun havde indbetalt det fulde investeringsbeløb, blev Greenfields Capi-tal ved med at ringe til hende meget ofte. Det blev hun irriteret over. I slutnin-gen af januar 2018 bad hun derfor Greenfields Capital om at overføre alle hen-des penge hos dem til hendes konto i Jyske Bank. De sagde, at pengene fra inve-steringskontoen først skulle tilbageføres til hovedbanken, inden de kunne over-føres til Jyske Bank.

Den 6. marts 2018 troede hun, at tilbagebetalingerne var sat i gang. Hun blev ringet op af en ny medarbejder, som arbejdede i den afdeling, hvor kunder blev afviklet. Han sagde, at han kunne se, at hun havde været kunde hos dem siden 2017, og at det var helt forkert, hvis hun ikke skulle have del i bonussen. Han sagde, at hvis hun betalte 4.000 euro, ville hun få bonussen udbetalt sammen med sit investeringsbeløb. Det, synes hun, var fint. Han ringede op til hende igen efter et par timer. Hun brugte sit dankort til overførslerne. Det lykkedes hende at overføre 1.000 euro to gange. De øvrige overførsler, hun forsøgte at lave, blev afvist. Hun sikrede sig, at der stod et tilstrækkeligt beløb på kontoen. Hun talte med medarbejderen, Person 2, hos Greenfields Capital i ca. en time og 20 minutter, fra kl. 15.33 til kl. 16.53. Han snakkede og snakkede. Han

talte bl.a. om sin barndom, sine bedsteforældre, og om hvor han kom fra i Rusland. Overførslerne skete, imens hun talte med ham. De talte ikke om, at hun skulle overføre et større beløb end 4.000 euro. Hun har ikke accepteret overførsel af beløb, der var større end 4.000 euro, og hun har ikke videregivet sine nøglekortoplysninger. Hendes nøglekort ligger ikke ved computeren. Hun har hentet det, når hun har skullet bruge det. Hun havde altid forud for den 6. marts 2018 fået tilsendt sms-koder, når hun skulle overføre beløb til Greenfields Capital. Også når hun brugte sit nøglekort. Hun skulle ikke bekræfte overførs-lerne den 6. marts 2018 med sms-koder. Hun ved ikke, hvordan overførslerne på 50.000 euro og 9.800 euro er foretaget. Hun har ikke lavet overførslerne.

Person 2 ringede til hende igen om aftenen, hvor hun talte med ham fra kl. 17.46 til kl. 17.52. Han virkede stresset og bad hende overføre de resterende to gange 1.000 euro fra en anden konto. Han skulle på kursus efterfølgende og ville gerne have afsluttet sagen med hende. Hun troede, at hun overførte to gange 1.000 euro, imens de talte sammen. De talte om, hvad hun tastede ind på computeren. På et tidspunkt, da der stod 1.000 euro til overførsel, sagde han ”push, push, push” . Hun har ikke ved en fejl skrevet 50.000 euro. Pludselig lagde Person 2 bare røret på. Person 2 ringede op igen kl. 18.01, hvor de talte sammen i ca. 3 minutter. Han bad hende om at kigge efter noget på computeren.

Den 9. marts 2018 konstaterede hun, at der var blevet trukket 50.000 euro og 9.800 euro på hendes konto. Hun kunne se, at pengene stod på hendes konto hos Greenfields Capital. Hun tænkte, at der var sket en fejl og bad Greenfields Capital om at tilbageføre beløbene. Hun blev opmærksom på, at der var tale om svindel, da Person 2 skrev til hende, at hun ikke kunne få sine penge til-bage på grund af tab, da dette jo ikke var i overensstemmelse med deres aftale om, at hun ikke kunne miste det grundbeløb, hun havde investeret.

Da hun kontaktede Jyske Bank, sagde de til hende, at hvis hun ikke selv havde foretaget overførslerne, ville banken dække tabet. De bad hende om at under-skrive en tro og love-erklæring. Hvis hun havde vidst, at hun og banken ikke havde samme interesse, ville hun ikke have udleveret alle bilagene med sine noter til banken, for det har været årsag til en del misforståelser.

Hun talte i telefon med Vidne 1 den 27. marts 2018. Han var rar og tålmodig. Hun vidste ikke, hvad der var foregået. Hvis han spurgte, om det kunne være foregået sådan og sådan, sagde hun bare ”ja” eller ”det kan godt være” . Hun var rystet og forvirret. Vidne 1 opfordrede hende til at få renset sin compu-ter og politianmelde forholdet. Hun gjorde begge dele med det samme. Der er ikke kommet noget ud af politiets efterforskning af sagen. Hun har selv gjort meget for at forfølge sagen. Hun har bl.a. skrevet til ombudsmanden, justitsmi-

nisteren, haft kontakt til politiet og en advokat i Hong Kong, politiet i Irland og dem, der står bag firmaet i Letland.

Foreholdt at hun i alt har overført 237.277 kr. til Greenfields Capital forud for den 6. marts 2018, og at hun har forklaret, at hun alene ville investere 135.000 kr., har hun forklaret, at hun ikke ved, hvorfor hun overførte så mange penge. Det var dumt af hende. Hun troede, at hun satte penge ind i en kapitalbank, hvorfra pengene kunne overføres til investeringskontoen. Hun troede, at der var tale om en almindelig bank.

Foreholdt ekstraktens side 185 og spørgsmålet om, hvornår hun forsøgte at overføre beløbene, har hun forklaret, at hun forsøgte at overføre beløbet på 4.000 euro af flere omgange via sit dankort den 6. marts 2018. De overførsler, hun forsøgte at lave kl. 15.56 og kl. 16.02 blev afvist. Hun forsøgte igen at over-føre yderligere to gange 1.000 euro ved bankoverførsel senere samme dag, da hun talte med Person 2.

Foreholdt ekstraktens side 163, mail af 9. marts 2018 til Person 2, har hun forklaret, at hun ikke kan huske, hvorfor hun ikke skrev til Person 2, at beløbene på 50.000 euro og 9.800 euro var blevet overført ved en fejl el-ler spurgte til, hvordan dette kunne være sket.

Foreholdt ekstraktens side 151, mail af 26. marts 2018 til Person 2, har hun forklaret, at hun på det tidspunkt havde indset, at han svindlede hende. Hun forsøgte at lokke oplysninger ud af ham.
Person 2 var ikke med på TeamViewer på hendes computer den 6.
marts 2018.

Vidne 1 har forklaret, at han er ansat i Jyske Bank. Han har bl.a. arbejdet med teknisk support hos Jyske Bank. I 2018 arbejdede han som sagsbehandler i Jyske Banks fraud-afdeling. Han arbejder stadig i fraud-afdelingen, men be-skæftiger sig i dag i højere grad med analyse og forebyggelse. Man skelner mel-lem autoriserede og uautoriserede overførsler. Oftest laver ofre ikke selv over-førslerne. I så fald er der tale om uautoriserede overførsler. I de typer af bedra-geri, hvor der sker autoriserede overførsler, bliver ofrene typisk manipuleret til selv at lave overførslerne. Han var sagsbehandler på Sagsøgers sag.

Foreholdt ekstraktens side 191, har han forklaret, at den øverste kasse på første side med datoen den 27. marts 2018 er et billede fra bankens notatsystem. Hans kollega, der havde den første kontakt med Sagsøger, har lavet no-tatet. De efterfølgende notater er fra sagsbehandlingssystemet. Han har skrevet nogle af notaterne. Han talte med Sagsøger den 27. marts 2018. Under "Info fra KS" står der, hvad hans kollega har skrevet. Hans eget notat fra

samtalen med Sagsøger står under ”Samtale med kunden” . Sagsøger sagde til ham, at hun ikke havde kontaktet b tidligere, fordi hun troede, at der var tale om en fejl, og fordi hun var i dialog med Greenfields Capital. De sætninger, der står i citationstegn, er direkte citering af det, som Sagsøger sagde til ham. Da han talte med Sagsøger, var der sat gang i at forsøge at få pengene ført tilbage fra modtagerens bank. Ud fra hans erfaring er det generelt afgørende, hvor hurtigt pengene søges retur fra modtagerens bank. Hvis man handler hurtigt, kan man have held med at få stoppet pengene, inden de kommer til modtagerens disposition. Det lykkedes dem ikke at få Sagsøgers penge tilbage.

Han opfordrede Sagsøger til at få renset sin computer, da Sagsøger havde forklaret til ham og hans kollega, at svindleren havde været med på TeamViewer på hendes computer. Man behøver ikke at slette no-get på computeren for at rense den.

Foreholdt ekstraktens side 190, har han forklaret, at det er atypisk, at en svind-ler lader et beløb på 73.000 kr. stå, hvis vedkommende har adgang til at foretage hævninger fra ofrets konto.

Det er usædvanligt, at der går 20 dage, fra et offer opdager misbrug, og til at banken gøres opmærksom på misbruget.

Han har tidligere arbejdet i borgerservice som vejleder indenfor NemID log og beskæftiger sig ofte med NemID logs i sit nuværende arbejde hos Jyske Bank.

Foreholdt ekstraktens side 180-184 med detaljer fra Sagsøgers Ne-mID logning, har han forklaret, at nummeret ud for ”kilde” er IP-adressen, der er anvendt af den bruger, der har lavet transaktionen. Det, der er anført ved ”Klient” , viser hvilken type enhed og browser, der er blevet anvendt.

Foreholdt sammenhængen mellem oplysningerne på side 180-181 og side 183-184, har han forklaret, at dette siger ham, at alle logningerne er lavet fra samme netværk og med samme internetudbyder. Det er normalt, at det sidste led i IP-adressen er varierende. Det handler om, hvordan man får tildelt IP-adressen. Man kan se, at der er tale om samme teleselskab og geografiske data, der var re-gistreret på IP-adresserne. For så vidt angår enheden, kan man ud fra klientop-lysningerne se, at logningen er sket fra en Windows-computer, men ikke om alle logningerne er foretaget fra samme Windows-computer.

På et tidspunkt i logningerne skifter tallet efter Chrome. De undersøgte, hvad der var årsag til, at oplysningerne skiftede fra Chrome/Nr. 1 til Chrome Nr. 2 og nåede frem til, at det kunne henføres til en opdatering af Chrome.

Foreholdt ekstraktens side 233, har han forklaret, at når man ser bort fra til-fælde, hvor gerningsmanden er i besiddelse af ofrets NemID-nøglekort, er der tre typer af svindel; phishing, keylogger og remote access tool. Phishing bliver oftest anvendt. I denne type sager sender gerningsmanden ofte en mail eller sms til ofret, som indeholder et link. Når ofret trykker på linket, kommer ved-kommende ind på en side, der for eksempel ligner Post Nords hjemmeside. Of-ret skal indtaste sine oplysninger, for eksempel betalings- eller NemID-oplys-ninger. Oplysningerne sendes til gerningsmandens system. Keylogger er den metode, der er set anvendt på biblioteker, hvor gerningsmanden via usb-stik kan se kundens indtastede oplysninger. Han tror ikke, at phishing- eller keylog-germetoden er anvendt i Sagsøgers situation, da svindleren i disse tilfælde typisk vil sætte deres egne tekniske spor, når de bruger ofrets op-lysninger. Svindel via remote access tool, som for eksempel TeamViewer, kræ-ver, at gerningsmanden har ofrets NemID-oplysninger. En svindler vil ikke kunne ændre beløbet i en overførsel.

Foreholdt ekstraktens side 228 og 229, har han forklaret, at dette påbud fra Fi-nanstilsynet vedrører hvidvask. Det drejer sig ikke om at forhindre en transak-tion, men om efterfølgende at vurdere, om der ved transaktionen var tale om hvidvask.

Foreholdt ekstraktens side 195, har han forklaret, at det er ham, der har oplistet beløbene for at skabe overblik i sagen. Der er anvendt sms-kode ved alle Sagsøgers overførsler til Greenfields Capital bortset fra de to omtvistede overførsler. Årsagen til dette er, at da de to omtvistede overførsler blev foreta-get, var der tidligere overført beløb til samme modtagerkonto, og der var efter-følgende gået noget tid, uden at de havde modtaget oplysninger om noget mistænkeligt. Derfor tænker systemet ikke, at der er tale om fraud og kræver ikke sms-godkendelse. Det er et kvalificeret gæt fra hans side, men det kan af-hænge af en lang række faktorer, som systemet tager i betragtning. Der sendes relativt sjældent sms-koder til godkendelse af transaktioner. Sms-koder har ikke noget med NemID eller 2-faktor godkendelse at gøre. Sms-koder sendes som en ekstra sikkerhedsforanstaltning fra Jyske Banks antifraud-system, når det vur-deres nødvendigt. Det er ikke et lovkrav.

Vidne 2 har forklaret, at han er ansat i Bankdata. Bankdata er en for-ening, der laver IT til 8 større pengeinstitutter i Danmark, herunder Jyske Bank. Han har en IT-faglig baggrund. Bankdata håndterede sikkerhed af netbank for Jyske Bank i 2018. NemID var sikkerhedssystemet i netbanken i 2018. Stærk kundeautentifikation er et spørgsmål om, at man skal have to ud af tre forskel-lige faktorer. De tre faktorer er noget man ved, noget man har, og noget man er. I 2018 var systemet indrettet sådan, at man kunne logge ind med bruger-id og adgangskode. Man kunne vælge at lave 2-faktor login, men det var ikke stan-

dard. Hvis man ville overføre penge, skulle man oplyse 2. faktor, for eksempel en kode fra et nøglekort, som det var tilfældet for Sagsøger. Når en kode fra nøglekortet er brugt, kan den ikke bruges igen. Hvis man har brugt en kode fra et nøglekort, og man umiddelbart efter skal foretage en overførsel mere, kan man bruge den session, man fik ved første nøgle. Dette lever op til kravet om 2-faktor godkendelse. Sessionskoden ligger på computeren og kan ikke bruges fra andre computere.

Foreholdt ekstraktens side 183, har han forklaret, at det er en log, som Nets bru-ger til NemID. Af beskrivelsen ud for "Hændelse" fremgår det, at der er tastet brugernavn, adgangskode og kode fra nøglekort.

Foreholdt ekstraktens side 184, hvor der ud for "Hændelse" bl.a. står 1-faktor login, har han forklaret, at det af beskrivelsen her fremgår, at der er tastet bru-gernavn og adgangskode men ikke tastet kode fra nøglekort. Beskrivelsen siger ikke noget om, at der er en session på computeren. Man kan ikke underskrive med 1-faktor login. Selvom der står 1-faktor login, er der reelt tale om et 2-fak-tor login, fordi sessionen fra det første 2-faktor login umiddelbart forinden kunne bruges som 2. faktor. Dette opfylder kravene til stærk kundeautentifika-tion.

Længden af sessionen afhænger af, om man laver noget hele tiden. Han kan ikke huske, hvor lang tid man skulle være inaktiv i 2018, før sessionsnøglen op-hørte. Ved PSD2-direktivet, som trådte i kraft i 2019, blev længden af den inak-tive tid nedsat til 5 minutter.

Foreholdt oplysningerne i bilag 1, side 2, har han forklaret, at det fremgår, at der er foretaget signering med nøglekort kl. 16.22.14. Der er logget ind på net-banken kl. 16.16.47.

Parternes synspunkter

Sagsøger har i det væsentlige procederet efter sit påstandsdoku-ment, hvori er anført følgende:

> "…
> Det gøres til støtte for den principale påstand **gældende** at Jyske Banks forpligtelser til at indrette sit kundeautentifikations- og screeningssy-stem, ikke er sket på tilstrækkelig sikker vis. Der henvises i den forbindelse til beskrivelsen af, hvorfor Jyske Bank ikke har opfyldt sine forpligtelser vedrørende kundeautentifikationen og screening af overførsler, samt til det i stævningen anførte på side 4 og 5.
>
> Det gøres **gældende,** at Jyske Bank på denne baggrund skal dække alle Sagsøgers fulde tab opgjort i den principale påstand jfr. Betalingslovens § 100, stk. 7.

I det omfang Retten finder, at Jyske Bank har opfyldt sine forpligtelser til stærk kundeautentifikation og screening af overførsler gøres det gældende, at Jyske Bank hæfter for Sagsøgers fulde tab jfr. Betalingslovens § 100, stk. 1.

Det gøres **gældende,** at Sagsøger har nægtet at have auto-riseret eller iværksat de i sagen omhandlede betalingstransaktioner, der førte til Sagsøgers tab. **Det bestrides,** at Sagsøger har anvendt sine personlige sikkerhedsforanstaltninger i forbin-delse med betalingstransaktionerne, og det gøres i den forbindelse lige-ledes **gældende,** at Sagsøger den 27. marts 2018 har un-derskrevet tro- og loveerklæring til Jyske Bank, hvoraf dette frem går.

Det gøres således **gældende** i medfør af betalingslovens § 98, stk. 2, at der ikke foreligger noget bevis for de påstande, som Jyske Bank har an-ført vedrørende benyttelse af sikkerhedsforanstaltningerne.

Det gøres samlet **gældende**, at det er Jyske Bank, der har bevisbyrden for, at der foreligger forhold, hvorefter Sagsøger selv skulle hæfte for sit tab helt eller delvist. Denne bevisbyrde har Jyske Bank ikke løftet. **Det bestrides,** at Sagsøger selv har fore-taget overførslerne, ligesom det **bestrides,** at Sagsøger på nogen måde har handlet svigagtig eller på anden måde ansvarspådra-gende.

Det **bestrides,** at tro- og love erklæringen er underskrevet for sent, såle-des som Jyske Bank har gjort gældende. I den forbindelse henvises til betalingslovens § 97. Det gøres **gældende,** at tidspunktet for, hvornår man afgav tro- og love erklæring, alene ville have haft betydning, idet der var sket yderligere misbrug efter det tidspunkt, hvor Sagsøger opdagede de to uberettigede overførsler på hhv. 50.000 euro og 9.800 euro. Det gøres ligeledes i den forbindelse **gældende,** at betalingslovens regler – her § 97 – er præceptive i forbrugerrelationer, hvorfor en eventuel bestemmelse i Jyske Banks kundeaftaler, der stiller Sagsøger ringere, end det der følger af loven, ikke er gæl-dende.

Jyske Bank har anført, at den omstændighed, at Sagsøger tidligere end den 7. marts 2018 havde foretaget investeringer skulle medføre, at Sagsøger efter Jyske Banks opfattelse har væ-ret uforsigtig eller på anden måde handlet, således at Jyske Bank ikke skal dække hendes tab. Disse antagelser **afvises,** og det **bestrides** i det hele, at det har nogen betydning for sagens bedømmelse, at Sagsøger tidligere har investeret midler via udenlandske selskaber.

Sagsøgers computer er blevet renset efter anmodning og anvisning fra Vidne 1 i Jyske Banks Fraud Afdeling. Jyske Bank har således, efter at misbruget var opdaget, rådgivet Sagsøger til at få fjernet muligheden for at fremfinde historikken i, hvad der er fo-retaget på computeren. Dette skal komme Jyske Bank til skade.

Jyske Banks antagelser om, at der ikke er andre muligheder for, at overførslen har kunnet finde sted, end at Sagsøger selv har fo-retaget disse, **bestrides** i sin helhed, og disse påstande og hypoteser fra Jyske Bank er fuldstændig udokumenteret. Det bemærkes, at Jyske Bank igennem alle sine processkrifter har forsøgt at mistænkeliggøre Sagsøger og dybest set anklager hende for at være krimi-nel. Sagsøger tager på det kraftigste afstand herfra. Hele forløbet omkring overførslerne den 7. marts 2018 (de uberettigede overførsler, som sagen drejer sig om) vil nærmere udførligt blive gennem-gået under forklaringerne under hovedforhandlingen.

De uberettigede transaktioner har kunnet finde sted, fordi Jyske Banks systemer ikke har sikret, at dette ikke kunne ske, og henset til at Green-fields Capitals medarbejdere har udført svindel. Hvorledes denne svin-del de facto er foregået kan være vanskeligt på nuværende tidspunkt at fastslå, bl.a. fordi Jyske Bank har rådgivet min klient om at lade alt på sin computer slette.

En af svindelmetoderne er, at den såkaldte RAT-metode, som er ud-bredt blandt svindlere, og som med stor sandsynlighed er den metode, hvor på Sagsøger er blevet svindlet. En sådan metode har den egenskab, at betaleren, d.v.s. i dette tilfælde Sagsøger, ikke har nogen mistanke om, at hvad der foregår, før det er for sent. Det bemærkes i øvrigt i den forbindelse, at Jyske Banks hængelås på hjemmesiden til log-in er en generisk hængelås, som nemt lader sig kopiere via RAT-metoden, hvor man bl.a. anvender falske hjemmesi-der. Dette vil nærmere blive beskrevet under proceduren i hovedfor-handlingen, og muligvis vil Vidne 2, Jyske Banks vidne, lige-ledes kunne medvirke til oplysning om, hvorledes RAT-metoden fak-tisk fungerer.

Jyske Bank har bl.a. gjort gældende, at Sagsøger er den der har den letteste og naturligste adgang til at sikre sig bevis for, at der ikke er sket uberettiget (svindel) overførsler. Dette er en ukorrekt anta-gelse fra Jyske Bank. Jyske Bank er klart den part, der har nemmest ved at bevise sine påstande. Jyske Bank har ikke løftet denne bevisbyrde el-ler på nogen måde sandsynliggjort, at Sagsøger skulle have handlet på en sådan måde, at Jyske Bank ikke hæfter for det tab, Sagsøger har lidt.

Det **bestrides** i sin helhed, at betalingslovens § 100, stk. 5 finder anvendelse, således som Jyske Bank har gjort gældende. Det **bestrides** i det hele, at Sagsøger har handlet uansvarligt eller i øvrigt har anvendt sin personlige sikkerhedsforanstaltning (Nem-ID) i forbindelse med overførslerne.

Såfremt Retten skulle være uenig heri, gøres det, som det fremgår af den subsidiære påstand, **gældende,** at der alene skal ske fradrag på kr. 375 i erstatning, som Sagsøger skal have udbetalt af Jyske Bank. Der henvises i den forbindelse til betalingslovens § 100, stk. 3, og under alle omstændigheder vil der maksimalt kunne ske fradrag på kr. 8.000 jfr. Betalingslovens § 100, stk. 4.

Under alle omstændigheder **bestrides** det som nævnt, at Sagsøger har handlet på en sådan måde, således at der skal ske fradrag i hendes udbetaling på erstatning, hverken fradrag jfr. Beta-lingslovens § 100 stk. 3 eller betalingslovens § 100, stk. 4.

Samlet gøres det **gældende,** at Sagsøger er blevet franar-ret sin personlige sikkerhedsforanstaltninger af Greenfields Capital, el-ler at Greenfields Capital på anden måde har kunnet sætte sig i besid-delse heraf. Jyske Bank har ikke godtgjort, at betingelserne for, at Sagsøger hæfter efter de udvidede ansvarsbestemmelser i beta-
lingslovens § 100. er opfyldt, og det gøres således **gældende,** at Jyske Bank skal betale erstatning svarende til det tab Sagsøger har lidt ved de uberettigede overførsler.
…"

Jyske Bank A/S har i det væsentlige procederet efter sit påstandsdokument, hvori er anført følgende:

"…

2.1 Sagens hændelsesforløb

Sagsøger kom i slutningen af 2017 i kontakt med et udenlandsk sel-skab, GreenFields Capital, som ifølge Sagsøger skulle foretage inve-steringer på hendes vegne. Hun havde herefter e-mail-korrespondance med selskabet i de følgende ca. 4 måneder, jf. Bilag A.

I perioden fra den 4. december 2017 og indtil de omtvistede betalinger blev foretaget den 6. marts 2018, foretog Sagsøger mere end ti over-førsler af samme karakter, som de omtvistede overførsler, dvs. over-førsler til udenlandske selskaber i investeringsøjemed, hvor Sagsøger efterfølgende anmodede Jyske Bank om at forsøge at få hendes overførsler tilbageført, jf. Bilag 4, s. 5. Overførslerne blev foretaget dels til GreenFields Capital eller selskaber, som ifølge Sagsøger selv frem-stod som foretaget til GreenFields Capital (EVG Trading Limited og Premium Peak), jf. stævningen (s. 2), dels til andre investeringsselska-ber, som det ikke er klart, hvorvidt fremstod som GreenFields Capital eller ej (idet Sagsøger ikke har besvaret Jyske Banks opfordring (c), jf. duplikken (s. 3)). For en oversigt over overførslerne henvises til Støtte-bilag A (dokumenteret ved Bilag E).

Det bemærkes, at Sagsøger ubestridt selv har foretaget alle de over-førsler, som fremgår af Støttebilag A, men bestrider at have foretaget de to i sagen omtvistede overførsler, jf. stævningen (s. 2), Bilag 4 (s. 2-3 og 5-7) og replikken (s. 1-2).

De af Sagsøger foretagne overførsler af samme karakter som de omt-vistede overførsler udgjorde i alt DKK 237.777,39, jf. Støttebilag A.

Efter den første overførsel til GreenFields Capital den 5. december 2017 spærrede Sagsøger sit Dankort, da GreenFields Capital kontaktede hende pr. telefon og mail og bad hende overføre flere penge. Ifølge Sagsøger gjorde denne henvendelse hende utryg ved situationen, jf. Sagsøgers klage til Det Finansielle Ankenævn (Bilag H, s. 2). Som det fremgår samme sted fortsatte Sagsøger imidlertid kontakten med og overførslerne til GreenFields Capital og andre investeringsselskaber. De mange overførsler, som ubestridt er foretaget af Sagsøger selv frem-går af Støttebilag A.

Den 6. marts 2018 forsøgte Sagsøger at overføre EUR 4.000 via kort-betaling, hvilket blev afvist, da beløbet oversteg det maksimale beløb, som kunne overføres via kortet. Sagsøger overførte herefter 2 x EUR 1.000, mens et fjerde forsøg på at overføre EUR 1.000 mere også blev af-vist som følge af, at betalingen oversteg maksimum. Overførslerne på 2 x EUR 1.000 blev foretaget klokken 15.59 og 16.00 og fremgår af kon-toudskrift indhentet fra Nets (Bilag B).

Sagsøger har anført, at overførslerne i Bilag B både blev foretaget som en "forsikring" for, at de tidligere indbetalte penge kunne blive ud-/tilbagebetalt (stævningen, s. 2) og for at Sagsøger kunne få udbetalt bonus (replikken, s. 3).

Samme dag, den 6. marts 2018, klokken 16.23, blev der foretaget en overførsel på EUR 50.000 fra Sagsøgers konto til GreenFields Capital. Overførslen blev godkendt ved indtastning af NemID-loginoplysninger (brugernavn og kodeord) samt NemID-nøglekortkode (den kode fra Sagsøgers fysiske papnøglekort, som passede til et automatisk og randomiseret udvalgt nummer på kortet), ligesom der af NemID blev udstedt en skjult sessionsnøgle, som blev lagret i kundens browser og kunne anvendes til efterfølgende betalinger i samme "flow".

Klokken 16.30 ligeledes den 6. marts 2018 blev foretaget endnu en over-førsel på EUR 9.800 fra Sagsøgers konto til GreenFields Capital. Overførslen blev godkendt ved brug af NemID-loginoplysninger (bru-gernavn og kodeord) samt anvendelse af den nævnte skjulte sessions-nøgle. Der blev således ikke anvendt NemID-nøglekortkode ved denne betaling, idet der i stedet blev anvendt en skjult sessionsnøgle (som gi-ver mulighed for at foretage flere betalinger i samme "flow" uden at skulle bruge en nøglekortkode hver gang, men samtidig opretholder betalingernes sikkerhedsniveau).

Det er disse to betalinger, som udgør sagens stridspunkt.

Jyske Banks elektroniske registreringer af gennemførelsen af overførs-lerne den 6. marts 2018 samt anvendelsen af NemID fremgår af Bilag 1 (overførslerne blev gennemført af systemet den 7. marts), og en forkla-ring vedrørende forløbet med betaling via NemID fra Vidne 2, IT Architect i Jyske Banks leverandør af ITsystem, Bankdata, frem-går af Bilag C.

Til overførslerne blev anvendt samme IP-adresse som blev anvendt ved tidligere overførsler af samme karakter, og Jyske Bank gør på denne baggrund gældende, at det er Sagsøgers IP-adresse, som er blevet anvendt i forbindelse med de omtvistede overførsler, jf. Bilag G og ud-dybende herom nedenfor i afsnit 3.2.3.

Efter overførslerne den 6. marts 2018 stod stadig et større beløb på cirka DKK 73.000 på Sagsøgers konto, jf. Bilag D.

Sagsøger havde efter de omtvistede overførsler korrespondance med repræsentanter fra GreenFields Capital i perioden fra den 9. marts 2018 til den 26. marts 2018, jf. Bilag A, hvor hun forsøgte at få tilbageført de to betalinger foretaget den 6. marts 2018 på EUR 50.000 og EUR 9.800.

Først den 27. marts 2018 kontaktede Sagsøger Jyske Bank, som spær-rede Sagsøgers NemID, netbank og betalingskort som følge af for-modning for investeringssvindel.

2.2 Parternes hovedanbringender

Sagsøger gør gældende, at overførslerne den 6. marts 2018 på EUR 50.000 henholdsvis EUR 9.800 er foretaget uden hendes medvirken, vi-den eller samtykke (stævningen, s. 2). Sagsøger gør samtidig gæl-dende, at hun ikke har videregivet sine NemID-oplysninger og/eller nøglekort (stævningen, s. 6) og at hun i det hele ikke har haft noget med overførslerne at gøre.

Jyske Bank gør heroverfor principalt gældende, at Sagsøger selv har foretaget de to af Sagsøger bestridte overførsler og dermed selv hæf-ter for det fulde beløb, jf. betalingslovens § 82 og modsætningsvis § 100, hvorefter hæftelsesreglerne i betalingslovens § 100 alene finder anven-delse ved uautoriserede betalinger, idet Sagsøgers forklaring om ikke at have videregivet sine NemID-oplysninger medfører, at overførs-lerne ikke kan være foretaget af andre end Sagsøger selv, når denne

forklaring sammenholdes med NemID-nøglekortets karakteristika som et fysisk papnøglekort samt de kendte metoder for svindel med NemID. NemID-nøglekortet kan således kun misbruges, hvis indehaveren selv medvirker ved at videregive nøglerne fra nøglekortet.

I tillæg hertil gør Jyske Bank gældende, at det taler for, at Sagsøger selv har foretaget overførslerne,

- *at* Sagsøger ubestridt foretog flere overførsler af samme karak-ter, herunder til samme selskab, i perioden op til de omtvistede overførsler;
- *at* der ikke blev gennemført yderligere overførsler efter de omtvi-stede overførsler, selvom der fortsat var et større beløb på kontoen (ca. DKK 73.000);
- *at* Sagsøgers IP-adresse blev anvendt til at foretage overførs-lerne;
- *at* Sagsøger ventede tre uger med at kontakte Jyske Bank, idet den naturlige adfærd efter at have fået stjålet næsten en halv mil-lion kroner ville være at kontakte sin bank straks efter at være ble-vet opmærksom herpå;
- *at* Sagsøgers korrespondance med GreenFields Capital i perio-den fra den 9. marts 2018 til den 26. marts 2018, taler for, at der har været tale om en frivillig investeringsoverførsel foretaget af Sagsøger selv; og
- *at* Sagsøger tidligere har forklaret, at hun selv har foretaget overførslerne mens repræsentanter fra GreenFields Capital var med på hendes computer via TeamViewer.

Såfremt retten mod forventning måtte finde, at Sagsøger ikke selv har foretaget de omtvistede overførsler, gør Jyske Bank **(i)** subsidiært gældende, at Sagsøger alligevel hæfter fuldt ud for beløbet, da Sagsøger indsigelse er indgivet for sent, jf. betalingslovens § 97, **(ii)** mere subsidiært gældende, at Sagsøger hæfter fuldt ud for beløbet, da Sagsøger med forsæt har oplyst sine NemID-oplysninger til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstæn-digheder, hvor Sagsøger indså eller burde have indset, at der var ri-siko for misbrug, jf. betalingslovens § 100, stk. 5, og **(iii)** mest subsidiært gældende, at Sagsøger hæfter for DKK 8.000, da Sagsøger enten har overgivet den personlige sikkerhedsforanstaltning med forsæt (uden at Sagsøger indså eller burde have indset, at der var risiko for misbrug, jf. § 100, stk. 5), eller Sagsøger ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse, jf. betalingslovens § 100, stk. 4.

Retten skal på baggrund af ovenstående således for det første tage stil-ling til, hvorvidt Sagsøger selv har foretaget de i sagen omtvistede overførsler, idet Sagsøger i dette tilfælde selv hæfter fuldt ud, jf. be-talingslovens § 82 og modsætningsvis § 100, hvorefter hæftelsesreglerne i betalingslovens § 100 alene finder anvendelse ved uautoriserede beta-linger. Hvis retten ikke finder, at Sagsøger selv har foretaget over-førslerne, skal retten tage stilling til, hvorvidt Sagsøger hæfter efter betalingslovens regler, som regulerer spørgsmålet om hæftelse i tilfælde af misbrug af betalingstjenester.

3. SAGEN FALDER UDEN FOR BETALINGSLOVENS ANVENDELSESOMRÅDE

De for denne sag relevante bestemmelser i betalingslovens regulerer den situation, hvor en person uberettiget har fået misbrugt en betalings-tjeneste, jf. betalingslovens § 82 og § 100, som omhandler uautoriserede betalinger, dvs. betalinger, hvor der ikke er givet samtykke. Jyske Bank gør principalt gældende, at Sagsøger selv har foretaget de to i sagen omtvistede overførsler, hvorfor sagen falder uden for betalingslovens anvendelsesområde, og Sagsøger derfor selv hæfter fuldt ud for de omtvistede overførsler. Dette uddybes i dette afsnit 3.

3.1 Sagsøgers forklaring sammenholdt med NemID-nøglekortets karakteristika samt kendte metoder til svindel medfører, at overførslen umuligt kan være foretaget af andre end Sagsøger selv

Sagsøger har anført, at hun ikke har videregivet sine NemID-oplys-ninger og/eller nøglekort og at hun ikke har haft noget med overførs-lerne at gøre eller kendskab til dem før efterfølgende (stævning, s. 6, vo-res understregning):

> "*Sagsøger ved ikke hvordan Greenfields Capital/EVG Trading Ltd har fået adgang til hendes loginoplysninger og oplysningerne på hendes nøg-lekort og kan derfor ikke forklare hvordan misbruget fandt sted. Sagsøger kan blot konstatere, at hun ikke har videregivet sine Nem- ID-oplysninger og/eller nøglekort, men at de tilsyneladende alligevel blev benyttet til at iværksætte 2 store omtvistede overførsler fra hendes konto…*"

På tidspunktet for de omtvistede betalinger krævede login i Jyske Banks netbank anvendelse af NemID-loginoplysninger (et brugerid og en adgangskode). Ved første betaling/overførsel krævedes NemID-bru-gernavn og -adgangskode samt kode fra det fysiske nøglekort. Ved log-

in blev der samtidigt lagret en skjult sessionsnøgle i kundens browser, så der kunne foretages yderligere betalinger (udover første betaling) ved brug af NemID-brugernavn og -adgangskode samt den skjulte ses-sionsnøgle i samme "flow" (uden brug af en kode fra det fysiske nøgle-kort), jf. Bilag C.

3.1.1 NemID-nøglekortets karakteristika

Det NemID-nøglekort, som er blevet anvendt i forbindelse med de omtvistede overførsler, er et fysisk papnøglekort. Det ligger dermed i selve nøglekortets karakteristika, at kortet kun kan misbruges, hvis indehave-ren selv medvirker til en overførsel enten ved selv at indtaste koderne eller ved at videregive koderne fra nøglekortet.

Da Sagsøger ifølge hende selv ikke har videregivet koderne fra nøg-lekortet, kan de omtvistede overførsler ikke være foretaget af andre end Sagsøger selv.

Der henvises i denne forbindelse til utrykt dom afsagt af Retten i Roskilde den 15. oktober 1987 i sag SS nr. 140/1987 B (sagen er trykt i Bryde Andersen: Edb-ret: lovgivning, retsafgørelser, kontrakter (1991), 1. udg., s. 128-129). Dommen angik en straffesag om overtrædelse af straffelovens § 165 om falsk anmeldelse.

I sagen fandt retten det godtgjort, at en Dankort-bruger selv havde fore-taget en række udtræk på sit Dankort, uagtet at han selv bestred dette. Selv om der var tale om en sag vedrørende kortbetaling, lægger retten vægt på forhold, som også har betydning i nærværende sag vedrørende betaling ved anvendelse af NemID. Af rettens præmisser fremgår såle-des (vores understregning):

> "*Retten skal udtale:*
> *I forbindelse med oprettelse af Dankort-systemet er der truffet en række sikkerhedsforanstaltninger for at forhindre, at der sker misbrug af kortet. Når henses til omfanget af disse foranstaltninger, herunder at man for at*
> *hæve på kortet skal benytte en personlig kode, findes det praktisk umuligt gentagne gange at hæve på kontoen uden kontohaverens medvirken. Når endvidere henses til at tiltalte har forklaret, at ingen andre end han kendte det personlige kodenummer, da han meget hurtigt lærte nummeret uden ad og destruerede det papir, hvor nummeret var anført på, findes den af tiltalte afgivne forklaring, om at han ikke har hævet på kontoen eller ladet en anden*
> *hæve på kontoen, at burde forkastes.*
> *Tiltalte findes derfor skyldig efter anklageskriftet.*

Som følge af det anførte vil tiltalte være at anse skyldig efter straffelovens § 165."

Ved oprettelsen af NemID-løsningen er der, ligesom for Dankort, truffet en række sikkerhedsforanstaltninger for at forhindre, at er sker misbrug af løsningen, herunder at man for at bruge løsningen både skal have vi-den om et individuelt brugernavn og kodeord samt have et fysisk nøg-lekort med engangskoder, som er ubrugelige efter, at de er blevet an-vendt.

Der kan i øvrigt henvises til Pengeinstitutankenævnets sag nr. 322/2014 (som også omhandlede kortbetaling), hvor ankenævnet fandt, at der ikke var grundlag for at antage, at der havde været tale om misbrug af et hævekort, men at hævningen i stedet var foretaget af kunden selv. Ankenævnet lagde vægt på, at kunden hele tiden selv var i besiddelse af sit hævekort, og at det således ikke var bortkommet.

Det er på denne baggrund umuligt at anvende NemID-løsningen til at foretage de omtvistede overførsler uden Sagsøgers medvirken. Når Sagsøger samtidig har forklaret, at hun ikke har videregivet sine Ne-mID-oplysninger og/eller nøglekort, kan overførslerne ikke være foreta-get af andre end Sagsøger selv.

3.1.2 Kendte metoder til svindel med NemID

Ovenstående understøttes af, at de tre kendte metoder til at begå svin-del med NemID (uden fysisk at have stjålet NemID-nøglekortet), kræ-ver en fysisk handling fra NemID-indehaveren: **(i)** ved phishing "fra-narres" en NemID-indehaver sine NemID-oplysninger, f.eks. ved at blive ledt ind på en falsk hjemmeside, hvor kunden indtaster sine Nem-ID-oplysninger (ved real time phishing spørger svindlerne via hjem-mesiden til en nøglekortkode, mens de simultant anvender koden til overførsel gennem deres egen computer), **(ii)** ved brug af en keylogger installeres et program på en NemID-indehavers computer, som "aflu-rer" pågældendes tastetryk (denne metode er mindre anvendelig i for-hold til NemID-nøglekortet, da en nøglekortkode kun kan bruges én gang), og **(iii)** ved brug af et Remote Access Tool (RAT, f.eks. TeamViewer) er svindlerne "med" på kundens computer og får kunden til selv at indtaste sine NemID-oplysninger.

I alle kendte metoder til svindel med NemID kræves således en fysisk medvirken fra NemID-indehaveren. Når det efter Sagsøgers forkla-ring kan lægges til grund, at hun ikke har videregivet sine NemID-op-

lysninger, er det også på denne baggrund umuligt, at overførslerne kan være foretaget af andre end Sagsøger selv.

3.1.3 Sagsøgers bemærkninger vedrørende svindelmetoden

Sagsøger anførte i replikken (s. 5 og 8-9), at svindlen skulle være sket således, at svindlerne "*ganske enkelt kopierer Jyske Banks hjemmeside, således at hverken Sagsøger eller nogen andre for den sags skyld vil kunne se forskel på den falske hjemmeside og Jyske Banks netbanks hjemmeside. Denne svindel kan foregå alene ved at svindleren fremsender ganske almindelig mail til kunden, evt. vedhæftet en PDF film."*

Jyske Bank bestrider, at svindlen kan være foregået på den af Sagsøger anførte måde. Hvis der var tale om svindel via en falsk hjem-meside, ville Sagsøger vide, at hun havde været inde på "Jyske Banks"− i så fald falske − hjemmeside og brugt sit nøglekort på det tids-punkt, hvor overførslen blev foretaget.

Sagsøger har imidlertid gentagne gange anført, at overførslerne blev foretaget "uden Sagsøgers medvirken, viden eller samtykke" (f.eks. stævningens s. 2), og Sagsøger slår således fast, at hun hverken at har været inde på "Jyske Banks" hjemmeside eller at har brugt sit nøgle-kort på overførselstidspunktet.

I forlængelse af ovenstående bemærker Jyske Bank, at Sagsøgers IP-adresse blev anvendt i forbindelse med de omtvistede overførsler, jf. Bi-lag G og uddybende herom nedenfor i afsnit 3.2.3.

Hvis overførslerne skulle være gennemført på den af Sagsøger be-skrevne måde, ville Sagsøger have tastet sin NemID-oplysninger ind på den falske Jyske Bank-hjemmeside, hvorefter NemID-koden ikke blev "brugt", men i stedet kunne anvendes af svindlerne til at foretage en overførsel (phishing eller real time phishing som beskrevet ovenfor). Når svindlerne så anvendte NemID-koden, ville dette ske fra svindler-nes computer og svindlernes netværk, hvorfor IP-adressen ville være en anden end Sagsøgers.

Overførslerne kan derfor ikke være gennemført som anført af Sagsøger og det fastholdes derfor, at den eneste mulighed er, at det er Sagsøger selv, som har foretaget overførslerne.

Jyske Bank bestrider i øvrigt, at svindlen kan være foregået ved at der er blevet fremsendt *"en ganske almindelig mail til kunden, evt. vedhæftet en PDF film"*, som Sagsøger også gør gældende.

Hvis svindlen skulle være sket via e-mail, ville denne e-mail ikke være blevet slettet ved en rensning af Sagsøgers computer. E-mails ligger således lagret på eksterne drev og ikke på computerens harddisk. Da Sagsøger ikke har fremlagt en e-mail af den i replikken anførte ka-rakter, gør Jyske Bank gældende, at en sådan e-mail ikke eksisterer. Som nævnt ville svindlen dog slet ikke kunne være foregået på denne måde, jf. ovennævnte om en falsk Jyske Bank-hjemmeside. Jyske Bank kan i øvrigt ikke se, hvad en fremsendt *"PDF-film"* skulle kunne hjælpe med ved svindlen.

Jyske Bank bemærker afslutningsvist, at Sagsøger under forberedel-sen har undladt at konkretisere Sagsøgers teori om, hvordan svind-len skulle være opstået, samt enkelte øvrige faktiske forhold. Sagsøger har derimod henvist til, at der vil blive redegjort nærmere herfor under hovedforhandlingen (Replikkens s. 5 og 6 og processkrift 1 s. 5). Sagsøger har således gjort det umuligt for Jyske Bank at forsvare sig imod disse ukendte synspunkter, som Sagsøger sagtens kunne have inddraget under forberedelsen. Jyske Bank protesterer derfor overfor, at Sagsøger får tilladelse til at fremkomme med disse uddybende an-bringender under hovedforhandlingen, i det de ikke bør tillades i med-før af retsplejelovens § 363.

Det er således umuligt, at overførslerne skulle kunne være sket på den af Sagsøger anførte måde. Overførslerne kan derfor kun være foreta-get af Sagsøger selv, som formentlig efterfølgende har fortrudt, at hun selv har overført de to euro beløb den 6. marts 2018 oveni alle de tidligere foretagne overførsler.

3.2 Sagens øvrige faktiske forhold tilsiger, at Sagsøger selv har foretaget overførslerne

I forlængelse af ovenstående og til støtte for Jyske Banks anbringende om, at Sagsøger selv har foretaget de omtvistede overførsler, gør Jy-ske Bank yderligere gældende, at hændelsesforløbet og Sagsøgers egne handlinger understøtter, at Sagsøger selv har foretaget de i sa-gen omtvistede overførsler.

3.2.1 Sagsøger har ubestridt foretaget flere overførsler af samme karakter i perioden op til de omtvistede overførsler

Sagsøger havde i en periode på tre måneder op til de omtvistede overførsler ubestridt foretaget mere end ti overførsler for i alt over DKK 230.000 af samme karakter, som de omtvistede overførsler, dvs. over-

førsler til udenlandske selskaber i investeringsøjemed, jf. Støttebilag A, dels ca. DKK 120.000 til GreenFields Capital eller selskaber, som frem-stod som GreenFields Capital (EVG Trading Limited og Premium Peak), dels over 100.000 til øvrige investeringsselskaber, som det ikke er klart, hvorvidt fremstod som GreenFields Capital eller ej (idet Sagsøger ikke har besvaret Jyske Banks opfordring (c), jf. duplikken (s. 3)). Dette taler for, at Sagsøger også selv foretog de to omtvistede over-førsler.

3.2.2 Der blev ikke gennemført yderligere overførsler, selvom der var flere penge på kontoen

Der blev ikke gennemført yderligere overførsler efter de omtvistede overførsler, selvom der fortsat var et større beløb på kontoen, jf. Bilag D, hvoraf fremgår, at der efter de to overførsler den 6. marts 2018 – og i øvrigt en måned frem, dvs. i hele perioden, hvor Sagsøger stadig kommunikerede med GreenFields Capital – fortsat var et stort indestå-ende på over DKK 70.000 på den konto, som beløbene blev overført fra.

Såfremt andre end Sagsøger skulle have været i besiddelse af Sagsøgers NemID-oplysninger, er det meget atypisk, at der ikke blev hævet yderligere beløb, idet en misbruger af f.eks. NemID typisk vil forsøge at hæve til kontoen er tom.

3.2.3 Sagsøgers IP-adresse blev anvendt til at foretage overførslerne

Den IP-adresse, som blev brugt til at foretage de omtvistede overførsler, er den samme IP-adresse, som blev brugt i relation til flere af de over-førsler, som Sagsøger har vedstået, at hun selv har foretaget (IP adresse 1 eller IP adresse 2). IP-adressen er registreret hos "*TDC: Denmark By Mobil Internet Access* ".

Der henvises i det hele til Jyske Banks log fra Sagsøgers henvendelse til banken (Bilag 4, s. 5-7) samt udtræk fra NemID-portalen (Bilag G), som indeholder en oversigt over tekniske oplysninger (herunder den anvendte IP adresse) vedrørende visse af de af Sagsøger ubestridt fo-retagne overførsler samt de to for sagen omtvistede overførsler.

Det kan således lægges til grund, at samme IP-adresse blev brugt til de to bestridte overførsler, som blev brugt til overførsler, som Sagsøger har erkendt. Dette taler også for, at Sagsøger selv har foretaget de to omtvistede overførsler.

3.2.4 Sagsøger ventede tre uger med at kontakte Jyske Bank

Sagsøger ventede med at kontakte Jyske Bank vedrørende de omtvi-stede overførsler til den 27. marts 2018, altså ca. tre uger efter overførs-lerne blev gennemført. Dette er et meget atypisk handlemønster, hvis Sagsøgers forklaring om, at overførslerne er foretaget uden hendes medvirken, viden eller samtykke, skulle være korrekt.

Hvis man som bankkunde åbner sin bankkonto og konstaterer, at der er foretaget overførsler for næsten en halv million kroner, og kunden ikke har nogen anelse om, hvordan overførslerne var foretaget, vil den helt sædvanlige fremgangsmåde for en bankkunde være straks at kontakte sin bank; ikke at vente tre uger.

Sagsøgers forklaring hænger altså ikke sammen, når hun anfører at være blevet opmærksom på de ifølge Sagsøger uberettigede over-førsler den 7. marts 2018, jf. Bilag 4 (s. 5), og herefter venter tre uger med at kontakte Jyske Bank.

Jyske Bank gør på denne baggrund gældende, at det må anses for en klar indikation på, at Sagsøger selv har foretaget overførslerne, at hun brugte tre uger på selv at forsøge at få pengene tilbage i stedet for straks at kontakte Jyske Bank. Det bemærkes i øvrigt, at overførslerne er foretaget fra Sagsøger og hendes mands fælleskonto, hvorfor der var to personer med adgang til kontoen, som ikke henvendte sig til banken for at få kontoen spærret.

Det bemærkes desuden, at jo længere tid, der går, fra overførslerne er foretaget, til banken bliver underrettet, jo mindre er bankens mulighe-der for at få overførslerne stoppet, idet det erfaringsmæssigt kan udle-des af de anmodninger om returnering, som banken foretager, at tid er en afgørende faktor. Det vil eksempelvis, alt efter type af overførsel, tage tid, før midlerne er til rådighed for modtager, ligesom der, alt efter beløbsstørrelse og modtagerbank, kan være begrænsninger på den dag-lige dispositionsret for modtager eller andre kontrolmekanismer, som forsinker dispositionen.

Der er især gode muligheder for at stoppe en overførsel inden for de første dage fra en overførsel er igangsat, og det er ikke usandsynligt, at Jyske Bank ville kunne have stoppet overførslerne, hvis Sagsøger havde kontaktet banken umiddelbart efter overførslerne var foretaget. Sagsøger har således ved at vente tre uger med at kontakte Jyske Bank selv forværret sine (og bankens) muligheder for at få pengene til-bage.

3.2.5 Sagsøgers korrespondance i perioden efter de omtvistede overførsler taler for, at hun selv har foretaget overførslerne

Sagsøgers korrespondance med GreenFields Capital i perioden fra den 9. marts 2018 til den 26. marts 2018 taler også for, at Sagsøger selv har foretaget overførslerne. Sagsøger skrev således bl.a. føl-gende i sine mails af 9. marts 2018 og 26. marts 2018 (Bilag A, s. 14 og 2):

> *"Now I have pressed the withdraw button to get our 60000Euro. Hope you will be able to send it back to our banc very quickly. How long time do you need to finish the rest.*
> *...*
> *Next time we trade it will be with my own capital. Answer me. Did you know.????? I am not stupid. I can see what a big opportunity you gave me. if my luck had been better. I use Team Viewer. What if the trading goes wrong. I have not the nerves to tackle the anger of my husband any longer. I did not want to involve you in this personal things but else you will not understand. Are you sure you can not send back the 60000E now?"*

Sagsøgers mails vedrørende de omtvistede overførsler indikerer så-ledes klart, at hun selv har foretaget overførslerne, da hun spørger, hvor lang tid den pågældende person fra GreenFields Capital skal bruge til at færdiggøre det resterende med det overførte beløb, at hun vil bruge sin egen kapital næste gang, de "handler", samt om GreenFi-elds Capital er sikre på, at de ikke kan sende pengene tilbage. Citatet synes at indikere, at det er ikke overførslerne, som Sagsøger er ked af, men at de er sket fra ægteparrets fælles konto.

3.2.6 Sagsøger har tidligere forklaret, at hun selv har foretaget overførslerne mens repræsentanter fra GreenFields Capital var med på hendes computer via TeamViewer

Da Sagsøger henvendte sig til banken den 27. marts 2018 oplyste hun, at der havde været nogle "med" på hendes computer via TeamViewer, jf. Jyske Banks log fra Sagsøgers henvendelse (Bilag 4, s. 5, vores understregning):

> *"Personen er med på kundens computer og på et tidspunkt er der proble-*
> *mer med kortet forklarer kunden, hvorefter personen foreslår en anden løsning.*
> *Hun husker ikke meget om, hvad der skete, men husker, at han sagde "push push push" .*

Hun siger:
Gud vide, om han har sagt, at jeg skulle tage mit nøglekort, det ved jeg faktisk ikke".
"Jeg vil ikke sige, at jeg ikke har hentet et nøglekort"

Herudover fremgår det både af klagesagen i Det Finansielle Ankenævn (bilag 5, s. 6) og Sagsøgers tro- og loveerklæring (bilag 2, s. 1), at Sagsøger har haft TeamViewer tændt.

Dette indikerer også, at Sagsøger selv har foretaget de i sagen omtvi-stede overførsler, jf. citatet ovenfor, hvor Sagsøger altså ikke vil ude-lukke, at hun selv har hentet sit nøglekort og overført pengene (mens en repræsentant fra GreenFields Capital har været med på computeren via TeamViewer).

3.3 Sammenfattende om, at Sagsøger selv har foretaget overførslerne

På baggrund af det i afsnit 3.1 og 3.2 anførte gør Jyske Bank gældende, at Sagsøger selv har foretaget de i sagen omtvistede overførsler og at Sagsøger dermed selv hæfter for overførslerne, idet betalingslovens regler om en banks hæftelse for overførsler foretaget fra en kundes konto kun vedrører den situation, hvor en kunde har fået misbrugt en betalingstjeneste og ikke den situation, hvor kunden selv har foretaget (autoriseret) en overførsel, jf. betalingslovens § 82 og modsætningsvis § 100, hvorefter hæftelsesreglerne i betalingslovens § 100 alene finder an-vendelse ved uautoriserede betalinger.

4. FULD HÆFTELSE FOR Sagsøger INDEN FOR BETALINGSLOVENS ANVENDELSESOMRÅDE

Hvis retten finder, at Sagsøger ikke selv har foretaget de omtvistede overførsler, falder sagen inden for betalingslovens anvendelsesområde, da betalingslovens § 97 og § 100 regulerer den situation, hvor en person uberettiget har fået misbrugt en betalingstjeneste, dvs. f.eks. hvis andre end en NemID-indehaver har anvendt NemID-indehaverens NemID-kort og -oplysninger, jf. betalingslovens § 82.

Hvis retten mod forventning finder, at Sagsøger ikke selv har foretaget de omtvistede overførsler, gør Jyske Bank **(i)** subsidiært gældende, at Sagsøger alligevel hæfter fuldt ud for beløbet, da Sagsøgers indsigelse er indgivet for sent, jf. betalingslovens § 97, **(ii)** mere subsidiært gældende, at Sagsøger hæfter fuldt ud for beløbet, da Sagsøger med forsæt har oplyst sine NemID-oplysninger til den, der har

foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor Sagsøger indså eller burde have indset, at der var risiko for misbrug, jf. betalingslovens § 100, stk. 5, og **(iii)** mest subsidiært gældende, at Sagsøger hæfter for DKK 8.000, da Sagsøger enten har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, med forsæt (uden at Sagsøger indså eller burde have indset, at der var risiko for mis-brug, jf. § 100, stk. 5), eller Sagsøger ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse, jf. betalingslovens § 100, stk. 4). Dette uddybes i det følgende.

4.1 Sagsøgers indsigelse er indgivet for sent og hun hæfter derfor for det fulde beløb

De i sagen omtvistede overførsler blev foretaget den 6. marts 2018 og Sagsøger kontaktede først Jyske Bank den 27. marts 2018, altså tre uger efter overførslerne blev foretaget, og desuden 20 dage efter den 7. marts 2018, hvor hun ifølge eget udsagn fik kendskab til overførslerne, jf. Bilag 1 (s. 5) (det bemærkes vedrørende sidstnævnte, at det er Jyske Banks opfattelse, at Sagsøgers medvirken har været nødvendig for at foretage overførslerne, jf. afsnit 4.2-4.3 nedenfor, og Jyske Bank er der-for af den opfattelse, at Sagsøger fik kendskab til overførslerne alle-rede den 6. marts 2018).

Jyske Bank gør på denne baggrund gældende, at Sagsøger har mistet sin ret til at gøre sin indsigelse om misbrug af NemID gældende, jf. be-talingslovens § 97.

Det fremgår af betalingslovens § 97, at indsigelser mod uautoriserede eller fejlbehæftede betalingstransaktioner skal være udbyderen i hænde, "*snarest muligt* " efter at betaleren har konstateret en sådan beta-lingstransaktion og senest 13 måneder efter debiteringen af den pågæl-dende betalingstransaktion. Jyske Bank gør gældende, at Sagsøger ved at vente 20 dage med at fremsætte sin indsigelse ikke har fremsat den "*snarest muligt* ".

Der henvises i denne forbindelse til Forbrugerombudsmanden notat af 25. november 2014 om indsigelsesfristen for uautoriserede og fejlbehæf-tede betalingstransaktioner i betalingslovens § 97 (opdateret 1. januar 2018) (s. 7), hvoraf fremgår, at en indsigelse indgivet inden for 14 dage vil opfylde betingelsen om "*snarest muligt* ". Dette må efter Jyske Banks opfattelse siges at være en meget vid udstrækning af begrebet " *snarest muligt* ", og da Sagsøger end ikke indgav sin indsigelse inden for 14

dage, må indsigelsen efter betalingslovens § 97 anses for at være indgi-vet for sent.

Det understreges desuden, at intet har forhindret Sagsøger i at tage kontakt til Jyske Bank i perioden på tre uger fra overførslerne blev fore-taget til Sagsøger faktisk tog kontakt til banken. Og på den anden side har Sagsøger ikke haft noget problem med at tage fat i GreenFi-elds Capital umiddelbart efter overførslen blev foretaget.

Sagsøger anførte i stævningen (s. 6), at det ikke skulle have betyd-ning, at Sagsøger først rettede henvendelse til Jyske Bank den 27. marts 2018, da tidspunktet for henvendelsen alene kunne have haft be-tydning, hvis der var sket yderligere misbrug efter det tidspunkt, hvor Sagsøger fik kendskab til de to uberettigede overførsler.

Dette bestrides, idet følgende fremgår af forarbejderne til betalingslo-vens § 97 (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 233, højre spalte, vores understregning):

> *"Selvom der efter bestemmelsen gælder en frist på højest 13 måneder til at gøre indsigelser gældende, kan brugeren af betalingstjenester fortabe denne ret på et tidligere tidspunkt på grund af passivitet, eksempelvis, hvis brugeren ved at der er foretaget en uautoriseret eller fejlbehæftet transaktionen og underlader at underrette udbyderen herom."*

Betalingslovens § 97 regulerer altså selve retten til at gøre indsigelser gældende og konsekvensen af bestemmelsen er dermed, at kunden hæfter for hele beløbet, hvis kunden ikke gør indsigelsen gældende "*snarest muligt* ".

I tillæg hertil bemærkes det, at det er muligt, at Jyske Bank kunne have stoppet overførslerne, hvis Sagsøger havde kontaktet Jyske Bank snarest muligt efter, at overførslerne var blevet foretaget, jf. afsnit 3.2.4 ovenfor. Det er således ikke, heller ikke rent faktuelt, uden betydning, at Sagsøger ventede tre uger med at kontakte banken.

Jyske Bank gør på baggrund af ovenstående gældende, at Sagsøger har mistet sin ret til at gøre sin indsigelse gældende, jf. betalingslovens § 97.

4.2 Sagsøger hæfter for det fulde beløb i henhold til betalings-lovens § 100, stk. 5

Hvis retten mod forventning finder, at Sagsøger har indgivet sin ind-sigelse rettidigt, gør Jyske Bank mere subsidiært gældende, at Sagsøger hæfter ubegrænset for de omtvistede overførsler, jf. betalingslo-vens § 100, stk. 5.

Betalingslovens § 100, stk. 5 er sålydende:

> *"Betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til beta-lingstjenesten hørende personlige sikkerhedsforanstaltning har været an-vendt 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."*

Den **første betingelse** for bestemmelsens anvendelse er, at den til beta-lingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt. Det fremgår af betalingslovens § 7, nr. 31, at en personlig sik-kerhedsforanstaltning er "[p]ersonaliserede elementer, som udbyderen stiller til rådighed for brugeren med henblik på at foretage autentifika-tion" og det fremgår direkte af forarbejderne til § 7, nr. 31, at NemID er et eksempel på en personlig sikkerhedsforanstaltning (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 106, højre spalte). Det fremgår af Bilag 1, at NemID er blevet anvendt til at godkende overførslerne, og betingelsen er dermed opfyldt.

Den **anden betingelse** for anvendelsen af betalingslovens § 100, stk. 5 er, at Sagsøger med forsæt har oplyst den personlige sikkerhedsfor-anstaltning til den, der har foretaget den uberettigede anvendelse. Som nævnt i afsnit 3.1 medfører selve NemID-nøglekortets karakteristika som et fysisk papnøglekort, at kortet kun kan misbruges af andre, hvis indehaveren selv medvirker ved at videregive nøglerne fra nøglekortet. Som nævnt samme sted kræver alle kendte metoder til at begå svindel med NemID, at kunden foretager en fysisk handling.

Det bemærkes i denne forbindelse, at det ikke (som ved fysisk kortbetaling) er muligt at "aflure" NemID-nøglekortoplysninger, som ifølge Sagsøger skulle være tilfældet, jf. stævningen (s. 6). NemID's nøglekort-koder er således engangskoder, som er ubrugelige, når de først er brugt én gang, og svindel med NemID fordrer således adgang til nøglekortet. I nærværende sag har repræsentanterne fra GreenFields Capital alene haft telefonisk og digital kontakt med Sagsøger, ligesom det på intet tidspunkt er konstateret, at nøglekortet har været væk.

Repræsentanterne fra GreenFields Capital kan på denne baggrund ikke have fået oplysningerne fra Sagsøgers NemID-nøglekort på anden måde, end at Sagsøger forsætligt har overgivet dette til dem (hvis retten altså finder, at det ikke er Sagsøger selv, som har foretaget overførslerne, jf. afsnit 3 ovenfor). Betingelsen er dermed opfyldt.

Den **tredje betingelse** for anvendelsen af betalingslovens § 100, stk. 5 er, at overgivelsen er sket under omstændigheder, hvor Sagsøger indså eller burde have indset, at der var risiko for misbrug.

På det tidspunkt, hvor overførslerne blev foretaget, havde Sagsøger kort forinden overført EUR 2.000 som "forsikring" for at få tilbagebetalt sine penge, jf. stævningen (s. 2). Hun må eller burde derfor på dette tidspunkt have indset risikoen for, at svindlerne misbrugte NemID-op-lysningerne, når hun overgav oplysningerne til dem, idet hun var villig til at overføre EUR 4.000 - næsten DKK 30.000 - og rent faktisk overførte EUR 2.000 – DKK 15.000 - som "forsikring" for at komme ud af et enga-gement.

Vedrørende det forhold, at Sagsøger efterfølgende igen foretog over-førsler (de omtvistede overførsler), selv om hun havde betalt for at komme ud af engagementet, henvises til at Sagsøger ifølge eget ud-sagt havde været utryg ved GreenFields Capital allerede i december 2017 og af den grund fik spærret sit Dankort, jf. Sagsøgers klage ved Det Finansielle Ankenævn (Bilag H, s. 2), men herefter fortsatte kontak-ten med og overførslerne til selskabet i flere måneder.

Det bemærkes, at Sagsøger i sagen ændrede forklaring og anførte, at "forsikringen" på EUR 2.000 blev betalt for at der kunne udbetales bonus og ikke for at tidligere indbetalte beløb skulle tilbagebetales, jf. replikken (s. 3).

Uanset om dette skulle være tilfældet, gør Jyske Bank gældende, at Sagsøger indså eller burde have indset risikoen for, at svindlerne mis-brugte NemID-oplysningerne, når hun overgav oplysningerne til dem.

Der henvises i den forbindelse til længden på den periode, som Sagsøger har haft kontakt til GreenFields Capital (tre måneder) samt at Sagsøger ifølge eget udsagn havde været utryg ved GreenFields Capital allerede i december 2017 og af den grund fik spærret sit Dankort, jf. Sagsøgers klage ved Det Finansielle Ankenævn (Bilag H, s. 2 (men her-efter altså fortsatte kontakten med og overførslerne til selskabet i flere måneder)).

I tillæg til ovenstående bemærker Jyske Bank, at det er en betingelse for, at Sagsøger hæfter efter § 100, stk. 5 (og desuden stk. 4, jf. nedenfor), at transaktionen er korrekt registreret og bogført, jf. betalingslovens § 100, stk. 1, 2. pkt. Jyske Bank gør gældende, at denne betingelse er op-fyldt og dokumenteret ved udskrifterne af Jyske Banks elektroniske re-gistreringer i betalingssystemet af overførslerne, jf. Bilag 1. Dette er i øvrigt ubestridt af Sagsøger.

Jyske Bank gør på baggrund af ovenstående gældende, at samtlige betingelser for at anvende betalingslovens § 100, stk. 5, er opfyldt og at Sagsøger derfor hæfter ubegrænset for det tab, som er opstået på baggrund af de to omtvistede overførsler. Jyske Bank skal derfor frifin-des for den af Sagsøger nedlagte påstand.

4.3 Sagsøger hæfter for DKK 8.000 efter betalingslovens § 100, stk. 4

Såfremt retten mod forventning måtte finde, at Sagsøger ikke hæfter ubegrænset, jf. betalingslovens § 100, stk. 5, gør Jyske Bank mest subsi-diært gældende, at Sagsøger hæfter for DKK 8.000 af det omtvistede beløb, jf. betalingslovens § 100, stk. 4, nr. 2 eller 3, da den til betalings-tjenesten hørende personlige sikkerhedsforanstaltning har været an-vendt, jf. afsnit 4.2 ovenfor, samt da Sagsøger enten har overgivet den personlige sikkerhedsforanstaltning med forsæt, jf. afsnit 4.2 oven-for (uden at Sagsøger indså eller burde have indset, at der var risiko for misbrug, jf. stk. 5), eller Sagsøger ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse. Der henvises i det hele til argumentationen nævnt i afsnit 4.2 ovenfor.

4.4 Betalingslovens § 100, stk. 8 finder ikke anvendelse

Jyske Bank bemærker afslutningsvis vedrørende betalingslovens § 100, stk. 4 og 5, at Sagsøger i stævningen (s. 6) gør gældende, at betalings-lovens § 100, stk. 8 finder anvendelse, hvorefter Sagsøger ikke hæf-ter, hvis tabet, tyveriet eller den uberettigede tilegnelse af det til beta-lingstjenesten hørende betalingsinstrument ikke kunne opdages af Sagsøger forud for den uberettigede anvendelse. Dette bestrides med henvisning til det i afsnit 3.1, 4.1 og 4.2 anførte, hvorefter det ikke er muligt, at den uberettigede tilegnelse ikke kunne opdages af Sagsøger, idet hun selv er nødt til at have været medvirkende til at over-give sine NemID-oplysninger. Jyske Bank gør på denne baggrund gæl-dende, at betalingslovens § 100, stk. 8, ikke finder anvendelse.

4.5 Jyske Bank har anvendt stærk kundeautentifikation og hæfter derfor ikke

Sagsøger gør gældende, at Jyske Bank hæfter som følge af, at Jyske Bank ikke har anvendt stærk kundeautentifikation ved overførslerne, jf. betalingslovens § 100, stk. 7 og stævningen (s. 4-5). Jyske Bank gør herover for gældende, at Jyske Bank har anvendt stærk kundeautentifika-tion.

Det fremgår af betalingslovens § 100, stk. 7, at betalingsudbyderen hæf-ter, såfremt denne ikke har krævet stærk kundeautentifikation. Bestem-melsen skal ifølge forarbejderne (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 239, venstre spalte) læses i sammenhæng med beta-lingslovens § 128, som fastslår, at der altid skal anvendes stærk kun-deautentifikation ved iværksættelsen af en elektronisk betaling (det be-mærkes, at § 128 i lovforslaget som fremsat var foreslået som § 127).

Som nævnt i afsnit 2.1 vedrørende sagens hændelsesforløb, blev den første af de to omtvistede overførsler (overførslen på EUR 50.000) gen-nemført ved anvendelse af NemID-login ved indtastning af både bru-gernavn og kodeord samt en kode fra nøglekortet, ligesom der blev ud-stedt en skjult sessionsnøgle, mens den anden transaktion på EUR 9.800 blev gennemført ved indtastning af NemID-brugernavn og -kodeord samt anvendelse af den netop forinden udstedte sessionsnøgle, da over-førslerne blev foretaget i samme "flow".

Betalingslovens § 7, nr. 30 definerer stærk kundeautentifikation som en autentifikation, som er baseret på anvendelsen af to eller flere elementer ("to faktor-godkendelse"), der er karakteriseret 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.

Det fremgår af forarbejderne til § 7, nr. 30 (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 106, højre spalte), at viden er karakteriseret som noget, som kun brugeren ved (f.eks. et kodeord) og at besiddelse er karakteriseret som noget, som kun brugeren besidder (f.eks. en NemID-engangskode). Det fremgår desuden direkte af forarbejderne til § 128 (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 275, højre spalte), at anvendelse af NemID til at gennemføre en kontoover-førsel fra netbank er et eksempel på stærk kundeautentifikation.

Jyske Bank gør på denne baggrund gældende, at der er anvendt stærk kundeautentifikation ved overførslerne.

Dette gælder begge overførsler, idet NemID brugernavn og kodeord (videns-element) og NemID-nøglekortkoden (besiddelseselement) ud-gjorde de to faktorer ved den første overførsel (EUR 50.000) mens Ne-mID brugernavn og kodeord (videns-element) og NemID-sessionsnøg-len (besiddelseselement) udgjorde de to faktorer ved den anden over-førsel (EUR 9.800), jf. også beskrivelsen heraf i Bilag C. Begge overførs-ler levede dermed op til kravet om to faktor-godkendelse.

Sagsøger gør gældende, at kravet om stærk kundeautentifikation ikke skulle være opfyldt som følge af, at Sagsøger ikke modtog en SMS-kode ved godkendelsen af betalingen, jf. stævningen (s. 5).

Dette er i nærværende sag uden betydning for, om kravet om stærk kundeautentifikation er opfyldt, idet betalingerne er gennemført ved brug af NemID og allerede derfor opfylder kravet om stærk kundeau-tentifikation (to faktor-godkendelse).

SMS-koden kunne udgøre den ene faktor i en to faktor-godkendelse, f.eks. ved online kortbetaling, hvor kortoplysningerne i så fald ville ud-gøre den anden faktor, men i nærværende sag er to faktor-godkendel-sen opfyldt allerede som følge af brug af NemID-loginoplysninger (bru-gernavn og kodeord) samt engangskoden fra NemID-nøglekortet hen-holdsvis den skjulte sessionsnøgle.

Jyske Bank gør på baggrund af ovenstående gældende, at Jyske Bank har anvendt stærk kundeautentifikation ved overførslerne.

4.5.1 Jyske Banks undertrykkelsesfunktion (Bilag 7) har ingen relevans for sagen

Sagsøger anførte i replikken (s. 11-12), at Bilag 7, som er en redegø-relse fra Finanstilsynet vedrørende Jyske Banks såkaldte undertrykkel-sesfunktion (funktionen forklares umiddelbart nedenfor), skulle tjene som bevis for, at Jyske Bank ikke har anvendt stærk kundeautentifika-tion. Jyske Bank bestrider, at dette skulle være tilfældet.

Jyske Banks undertrykkelsesfunktion nævnt i Bilag 7 er en funktionali-tet, der bruges til at undertrykke alarmer på kunder, der anvender ban-ken på en for dem naturlig og legal måde, men hvis transaktioner dan-ner alarmer i bankens overvågningsscenarier. De alarmer, som dannes i bankens kontantovervågningsscenarier ved sådanne kunders kontan-tindsættelser, kan undertrykkes i en kortere periode, således at de ikke skal undersøges manuelt af en medarbejder.

Bankens overvågningssystem fungerer på den vis, at det screener kun-dernes transaktioner efter, at transaktionerne er foretaget og gennem-ført. De alarmer, der dannes i overvågningssystemet, har Jyske Bank via sin undertrykkelsesfunktion mulighed for at undgå at få ud til manuel behandling.

Funktionen anvendes på de kunder, som banken har et dybdegående kendskab til, men hvis forretningsmodel for eksempel indebærer regel-mæssige større kontantindsættelser, eksempelvis fra den daglige om-sætning i et større supermarked. Den overvågning, som undertrykkel-sesfunktionen angår, er således en efterfølgende overvågning og har in-gen betydning i nærværende sag.

Jyske Bank kan i øvrigt oplyse, at undertrykkelsesfunktionen nævnt i Bilag 7 aldrig har været anvendt på en overførsel foretaget af Sagsøger, og at systemet dermed ikke har undertrykt nogen alarmer vedrø-rende overførsler foretaget af Sagsøger.

Finanstilsynets redegørelse - og den overvågningsfunktion, som det vedrører - har således ingen relevans i nærværende retssag, og Jyske Bank gør på denne baggrund gældende, at Bilag 7 ikke har noget som helst at gøre med Jyske Banks forpligtelse til at anvende stærk kun-deautentifikation.

5. BEVISBYRDE

5.1 Sagsøger har bevisbyrden for, at der er sket uberettiget brug, jf. betalingslovens § 98

Jyske Bank gør gældende, at Sagsøger har bevisbyrden for, at hun ikke selv har foretaget de omtvistede overførsler, jf. betalingslovens § 98.

Betalingslovens § 98 er sålydende (vores understregning):

> *"Hvor en betaler nægter at have autoriseret eller iværksat en betalings-transaktion, har udbyderen af betalingstjenesten bevisbyrden for, at beta-lingstransaktionen er korrekt registreret og bogført og ikke er ramt af tek-niske svigt eller andre fejl, jf. dog stk. 3. Ved brug af et betalingsinstru-ment har udbyderen endvidere bevisbyrden for, at den til betalingsin-strumentet hørende personlige sikkerhedsforanstaltning er blevet anvendt i forbindelse med betalingstransaktionen.*

Stk. 2. Hvor en betaler nægter at have autoriseret eller iværksat en beta-lingstransaktion, er registrering af brug af betalingsinstrumentet ikke i sig selv bevis for, at betaleren har godkendt transaktionen, at betaleren har handlet svigagtigt, eller at betaleren har undladt at opfylde sine for-pligtelser."

Betalingslovens § 98, stk. 1, bestemmer således vedrørende bevisbyr-den for, at betalingslovens § 97 og § 100 om misbrug af betalingstjene-ster finder anvendelse, at hvor en betaler nægter at have autoriseret el-ler iværksat en betalingstransaktion, har udbyderen af betalingstjene-sten (dvs. Jyske Bank) bevisbyrden for, at betalingstransaktionen er kor-rekt registreret og bogført og ikke er ramt af tekniske svigt eller andre fejl.

Jyske Bank gør gældende, at Jyske Bank har løftet denne bevisbyrde ved udskrifterne af Jyske Banks elektroniske registreringer i betalings-systemet af overførslerne, jf. Bilag 1. Det bemærkes i øvrigt, at det ikke bestrides af Sagsøger, at transaktionerne er korrekt registreret og bogført.

Betalingslovens § 98, stk. 2 bestemmer, at hvis Jyske Bank har løftet sin bevisbyrde efter stk. 1, er selve registreringen af, at NemID'et er blevet brugt ikke *i sig selv* bevis for, at Sagsøger har godkendt transaktio-nen, handlet svigagtigt, eller har undladt at opfylde sine forpligtelser. Betalingslovens § 98, stk. 2, bestemmer dermed alene, at det forhold, at Jyske Bank har løftet sin bevisbyrde vedrørende korrekt registrering i stk. 1, ikke automatisk medfører, at Sagsøger skal anses for at have foretaget de to omtvistede overførsler.

Bestemmelsen siger imidlertid ikke herudover noget om bevisbedøm-melsen, som må foretages på baggrund af sagens omstændigheder i øv-rigt, jf. bestemmelsens forarbejder (lovforslag nr. 157 af 15. marts 2017, FT 2016-17, tillæg A, s. 234, højre spalte, vores understregning):
"Denne bestemmelse finder ifølge sin ordlyd kun anvendelse på beta-lingsinstrumenter og fastslår, at selve brugen af et betalingsinstrument ikke kan betragtes som bevis for de forhold, der er beskrevet i bestemmel-sen. Brug af et betalingsinstrument kan derimod godt indgå som et led i bevisbedømmelsen i en sag, hvor det skal vurderes, om betaleren har handlet svigagtigt.

Bestemmelsen indfører herudover ikke regler for bevisbedømmelsen. Hvis en bruger af betalingstjenester bestrider at have brugt et betalingskort, uanset at udbyderen kan bevise, at kortet og den til kortet hørende per-

sonlige sikkerhedsforanstaltninger har været anvendt i forbindelse med betalingstransaktionen,
vil det derfor være op til det relevante ankenævn, eksempelvis pengeinsti-tutankenævnet eller teleankenævnet, eller domstolene at tage stilling til, om brugen af kortet kan anses for foretaget af brugeren på baggrund af
sagens omstændigheder."

Som det fremgår af forarbejderne til bestemmelsen, indfører § 98, stk. 2 ikke regler for bevisbedømmelsen, udover at registrering af brug af betalingstjenesten ikke i sig selv er bevis for, at betaleren har godkendt transaktionen.

Jyske Bank gør netop gældende, at Sagsøger selv har foretaget over-førslen med henvisning til brugen af NemID, herunder NemID's karak-teristika, sammenholdt med sagens øvrige omstændigheder, herunder Sagsøgers egen forklaring om, at hun ikke har videregivet sine Ne-mID-oplysning og/eller nøglekort og i øvrigt ikke ved, hvad der er sket, samt sagens øvrige faktiske forhold, som tilsiger, at Sagsøger selv har foretaget betalingerne. Jyske Bank har således netop fremført yder-ligere forhold end kun det forhold, at betalingstjenesten er blevet brugt, og alle disse forhold tilsiger, at Sagsøger selv har foretaget betalin-gen.

Herudover gælder de almindelige bevisbyrderegler, hvorefter der ved vurderingen af bevisbyrden tages hensyn til, dels hvilken part, der havde den letteste og naturligste adgang til at sikre sig beviset, og dels at den part, der påstår noget usædvanligt i forhold til sædvanlige aftale-og kontraktvilkår, må bevise det, jf. Gomard og Kistrup: Civilprocessen (2020), 8. udg. (s. 565-566), og Dahlager: Civile retssager (2015), 2. udg. (s. 147).

Jyske Bank gør gældende, at Sagsøger har haft den letteste og natur-ligste adgang til at sikre sig beviset, idet Sagsøger har været eneste involverede person, og at banken kun har de elektroniske udskrifter, som allerede er fremlagt i Bilag 1 (dette må desuden anses for baggrun-den for, at bevisbyrdereglen i betalingslovens § 98 er formuleret, som den er; at banken kun har bevisbyrden for, at overførslen er korrekt re-gistreret og bogført og ikke er ramt af tekniske svigt eller andre fejl).

Jyske Bank gør desuden gældende, at Sagsøger påstår noget usæd-vanligt, idet sagens faktiske forhold tilsiger, at hun selv har foretaget overførslerne, jf. afsnit 3.1 og 3.2 ovenfor.

I tillæg hertil henvises til dom afsagt af Københavns Byrets den 11. november 2013, der vedrører den tidligere bestemmelse i § 62 i lov om betalingstjenester og elektroniske penge, som svarer til § 100 i betalingsloven (s. 16, vores understregning):

> *"Efter vidnet, M's, forklaring på baggrund af listen over transaktioner foretaget på sagsøgers MasterCard i perioden 15. september 2011 til den 23. september 2011 lægger retten til grund, at de omtvistede transaktioner på i alt 98.912,12 kr. er sket under anvendelse af MasterCardets chip og korrekt PIN-kode.*
>
> *Det påhviler herefter sagsøger at påvise, at der forelå en uberettiget anvendelse af betalingskortet, jf. § 62 i lov om betalingstjenester og elektroniske penge."*

Sagsøger var i sagen en bankkunde, der gjorde gældende, at han var blevet udsat for misbrug af sit MasterCard, ligesom Sagsøger gør gældende vedrørende NemID i nærværende sag. Retten fandt, at Ma-sterCardets chip og korrekt PIN-kode var blevet anvendt, og at det her-efter påhvilede kortindehaveren at føre bevis for, at der havde fundet misbrug sted. Der henvises i denne forbindelse desuden til Jan Trza-skowski m.fl.: Internetretten (2017), 3. udg. (s. 542-543), hvoraf fremgår:

> *"Hvis udbyderen [Jyske Bank] findes at have godtgjort, at en transaktion er korrekt bogført og registreret, jf. betalingslovens § 100, stk. 1, 2. pkt., jf. § 98, stk. 1, påhviler det betaleren [Sagsøger] at bevise – som betin-gelse for anvendelse af ansvars- og tabsbegrænsningsreglerne i § 100 – at der har fundet "uberettiget anvendelse" af betalingsinstrumentet sted. Har betaleren selv – eller nogen med hans bemyndigelse – initieret den debiterede transaktion, hæfter betaleren fuldt ud, jf. ovenfor." Mine tilfø-jelser i "[ ]".*

Jyske Bank gør på baggrund af ovenstående gældende, at Sagsøger har bevisbyrden for, at der har fundet misbrug sted, samt at Sagsøger på baggrund af det i afsnit 3 anførte ikke har løftet denne bevis-byrde. På denne baggrund finder hæftelsesreglerne i betalingslovens § 100 ikke anvendelse, hvorfor Jyske Bank som nævnt ikke kan hæfte for de overførte beløb og derfor skal frifindes for den af Sagsøger ned-lagte påstand.

5.2 Sagsøgers bemærkninger vedrørende Jyske Banks ageren er ikke korrekte og i øvrigt uden relevans for sagen

Sagsøger betvivlede både i replikken (s. 4 og 9-10) og i sit afsluttende processkrift (s. 3) Jyske Banks behjælpelighed i forbindelse med at få de i sagen omtvistede beløb tilbage til Sagsøger, ligesom Sagsøger i replikken (s. 4) anførte, at Jyske Bank har rådgivet Sagsøger til at få renset sin computer og at Jyske Bank dermed har "*medvirket til at fjerne yderligere dokumentation af hændelsesforløbet og hvorledes svindlen fra Green-fields Capital er foregået".*

Hertil bemærker Jyske Bank indledende, at Jyske Bank ikke kan se disse bemærkningers relevans for sagens substans, men det synes ifølge Sagsøger at relatere sig til bevisbyrden, idet Sagsøger altså har an-ført, at Jyske Banks ageren skulle have ført til, at visse beviser i sagen ikke eksisterer. Jyske Bank vil derfor nedenfor kort redegøre for Jyske Banks ageren i sagen, idet det bestrides at Jyske Bank ikke har været be-hjælpelige, ligesom det bestrides, at der skulle være beviser i sagen, som ikke eksisterer, idet Sagsøger ikke har redegjort for hvilke bevi-ser, der skulle være at finde på hendes computer, som er blevet fjernet
ved rensningen af Sagsøgers computer. Herudover bestrides det - for det tilfælde, at der skulle være beviser, som ikke eksisterer − at det skyldes forhold, som kan tilskrives Jyske Bank, at sådanne beviser ikke eksisterer.

Vedrørende Jyske Banks behjælpelighed har Jyske Bank foretaget alle de skridt, som Jyske Bank kunne for at få de omtvistede beløb tilbage. Der henvises til, at Jyske Bank allerede fra den 28. marts 2018 (altså da-gen efter Sagsøger henvendte sig til banken) via SWIFT-meddelelser til forbindelsesbanken Deutsche Bank har haft forbindelse til modtager-banken DBS Bank i Hong Kong, og anmodet om, at overførslerne tilba-gekaldes, jf. Bilag F. Herudover har Jyske Bank haft adskillige samtaler med Sagsøger fra hun henvendte sig den 27. marts 2018 frem til 18. december 2018, hvor banken på forskellig vis har forsøgt at hjælpe Sagsøger, jf. i det hele Bilag 4. Jyske Bank bemærker i denne henseende i øvrigt, at Sagsøger selv har forværret mulighederne for, at Jyske Bank ved sine henvendelser til Deutsche Bank og DBS Bank kunne få pengene tilbageført, idet Sagsøger først henvendte sig til Jyske Bank tre uger efter overførslerne var foretaget, jf. afsnit 3.2.4 ovenfor.

Vedrørende spørgsmålet om rensning af Sagsøgers computer be-mærker Jyske Bank, at såfremt en kunde har været i kontakt med for-modede kriminelle og potentielt har givet dem adgang til sin computer (f.eks. via TeamViewer, som Sagsøger indledende oplyste til banken var tilfældet) eller til at installere programmer eller såfremt der er mi-stanke herom, så er det best practice – og helt logisk – at anbefale, at

kunden sikrer, at der ikke er uvedkommende, der (fortsat) har uret-mæssig adgang til de relevante enheder, før de anvendes igen. Dette henset til, at der ellers er risiko for, at denne adgang kan misbruges.

Jyske Bank oplyser i den forbindelse kunden om, at kunden skal have enhederne renset eller nulstillet/formateret men først efter, at kunden har spurgt myndighederne, om de ønsker at undersøge for eventuelle beviser. Alternativt kan man helt undlade at anvende enhederne og sikre dem som beviser.

Hvilken løsning kunden vælger, er helt op til kunden og ikke noget, Jy-ske Bank blander sig i, men det er vigtigt, at kunden er opmærksom på, at det er noget, som kunden skal forholde sig til som en del af at "standse ulykken" . Det er denne besked, Sagsøger har fået, idet hun ved henvendelsen til banken oplyste, at der har været en eller flere per-soner med på hendes computer for at hjælpe hende med at investere.

Herudover bemærker Jyske Bank i øvrigt vedrørende hændelsesforlø-bet og rensning af Sagsøgers computer, at Sagsøger henvendte sig første gang til Jyske Bank den 27. marts 2018, hvor hun blev anbefalet politianmeldelse (Bilag 4, side 5).

Sagsøger kontaktede Jyske Bank igen den 3. april 2018, da hun var blevet kontaktet af svindlerne igen (mellem den 27. marts 2018 og 3. april 2018) og havde fået oplyst, at hun kunne få ført EUR 40.000 til-bage, hvis Sagsøger lod svindlerne være med på TeamViewer (hvil-ket er baggrunden for, at Sagsøger blev anbefalet at rense sine enhe-der).

Sagsøger blev således henvist til politiet en uge forinden hun var ble-vet anbefalet at rense sin computer, og politiet kunne have oplyst Sagsøger om, at hun skulle vente med at rense sine enheder.

Herudover fremgår det af Bilag 4 (s. 1-2), at Sagsøger først oplyste til Jyske Bank, at hun havde været til teknikker og fået skiftet sin harddisk den 18. december 2018, altså længe efter hun både havde været hos banken og politiet (og i øvrigt advokat, som også kunne have oplyst hende om at sikre eventuelle beviser, og som hun henvendte sig til før den 11. april 2018, jf. Bilag 4 (s. 4)). Det er altså tvivlsomt, om Sagsøger overhovedet har fået renset sin computer før længe efter Jyske Bank anbefalede at rense hendes computer og på et tidspunkt, hvor både politi og advokat kunne have sikret beviser.

I forlængelse heraf bemærker Jyske Bank, at Sagsøger ved kontakten til banken den 18. december 2018 oplyste, at hun havde haft sin compu-ter inde hos en teknikker, der havde skiftet harddisken. Jyske Bank un-drer sig over, at teknikeren i så fald ikke tog kopi af harddisken eller at Sagsøger ikke stadig har den tidligere harddisk, som blev skiftet ud.

Jyske Bank har i duplikken (s. 6) ved opfordring (f) forsøgt at få Sagsøger til at redegøre for og dokumentere, hvornår hun har fået renset sin computer. Sagsøger har ikke besvaret denne opfordring, men i processkrift 1 (s. 4) blot anført, at "*Sagsøger fik som anført ovenfor renset sin computer umiddelbart efter svindlen eller i hvert fald kort tid derefter.* " Jy-ske Bank anser hverken opfordringen for besvaret eller udsagnet for dokumenteret og gør gældende, at retten dermed kan lægge til grund, at Sagsøger først fik renset sin computer på et senere tidspunkt om-kring den 18. december 2018, jf. bilag 4 (s. 1-2), og altså længe efter, at hun havde været hos banken og desuden på et tidspunkt, hvor hun havde været ved både politi og advokat, som kunne have sikret eventu-elle beviser (såfremt sådanne måtte eksisterer, hvilket Jyske Bank altså også bestrider, jf. indledningen til nærværende afsnit 5.2).

Jyske Bank bemærker og understreger dog, at det fortsat ikke fremgår af Sagsøgers processkrifter, hvilken betydning dette skulle have for den retlige bedømmelse af sagen.
…"

Rettens begrundelse og resultat
Sagsøger har gjort gældende, at to udenlandske transaktioner fra hendes konto i Jyske Bank foretaget den 6. marts 2018 kl. 16.23.31 og kl. 16.30.05 på henholdsvis 50.000 euro og 9.800 euro til EVG Trading Limited ikke er auto-riseret af hende, og at Jyske Bank A/S derfor hæfter for det tab, hun har lidt som følge af tredjemands uberettigede overførsel af beløbene, jf. betalingslovens § 100.

Af betalingslovens § 82, stk. 1, fremgår, at en betalingstransaktion kun er autori-seret, hvis betaleren har meddelt samtykke til at gennemføre transaktionen. En betalingstransaktion anses for uautoriseret, hvis der ikke er meddelt samtykke.

Det fremgår at betalingslovens § 98, stk. 1, at hvis en betaler nægter at have au-toriseret eller iværksat en betalingstransaktion, har udbyderen af betalingstje-nesten bevisbyrden for, at betalingstransaktionen er korrekt registreret og bogført og ikke er ramt af tekniske svigt eller andre fejl, jf. dog stk. 3. Ved brug af et betalingsinstrument har udbyderen endvidere bevisbyrden for, at den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning er blevet anvendt i forbindelse med betalingstransaktionen. Registrering af brug

af betalingsinstrumentet er efter bestemmelsens stk. 2, 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.

På baggrund af de fremlagte udskrifter fra Jyske Banks elektroniske registrerin-ger af transaktionerne lægger retten til grund, at betalingstransaktionerne er korrekt registreret og ikke er ramt af tekniske svigt eller andre fejl.

Retten lægger efter logoplysningerne, der er understøttet af forklaringen fra Vidne 2, videre til grund, at der i forbindelse med de to transaktioner er anvendt 2-faktor godkendelse, idet der ved transaktionen foretaget kl.
16.23.31 er anvendt en adgangskode og en nøgle fra et nøglekort eller en kode-viser, og at der inden for samme session er anvendt en adgangskode til transak-tionen kl. 16.30.05.

Sagsøger har forklaret, at hun ikke har anvendt sit NemID i for-bindelse med de to overførsler, og at hun ikke har videregivet oplysningerne fra sit nøglekort. Hun har videre forklaret, at medarbejderen fra Greenfields Capi-tal ikke var med på TeamViewer, da overførslerne blev foretaget.

Det kan lægges til grund, at Sagsøger på trods af sin intention om alene at investere 135.000 kr. over en periode fra den 3. december 2017 til den 6. marts 2018 umiddelbart op til de to omtvistede overførsler har foretaget 11 ind-betalinger og samlet investeret for ca. 212.000 kr. Hun har erkendt, at hun den 6. marts 2018 – kort forinden de omtvistede overførsler – to gange overførte 1.000 euro, uagtet at hun ønskede at afslutte arrangementet. De to overførsler på 1.000 euro er foretaget fra samme IP-adresse og med de samme oplysninger om anvendt styresystem, browser, teleselskab og geografisk lokation i Danmark, som de to omtvistede overførsler.

På den baggrund og sammenholdt med Sagsøgers forklaring om karakteren af telefonsamtalerne med medarbejderen fra Greenfields Capital den 6. marts 2018 og indholdet af den efterfølgende mailkorrespondance, at hun ikke før den 27. marts 2018 henvendte sig til Jyske Bank og oplyste, at der var tale om uautoriserede overførelser, samt forklaringen fra Vidne 1 om hans notater i Jyske Banks system fra samtalen med Sagsøger, lægger retten til grund, at betalingerne er sket med Sagsøgers medvirken og samtykke. Det er herefter ikke godtgjort, at der er tale om uautoriserede overførsler.

Den omstændighed, at Sagsøger meget sikkert har forklaret, at hun ikke har godkendt de to transaktioner med sit NemID, at hun efterfølgende har underskrevet en tro- og love erklæring, og at hun formentlig er blevet mani-puleret til at foretage overførelserne, kan ikke føre til et andet resultat.

Da hæftelsesreglerne i betalingslovens § 100 alene finder anvendelse på uautoriserede betalinger, tager retten derfor Jyske Banks påstand om frifindelse til følge.

Sagsøger har tabt sagen og skal betale sagsomkostninger til Jyske Bank A/S.

På baggrund af sagens værdi, omfang og forløb fastsættes sagens omkostninger til 50.000 kr. Beløbet, der er til dækning af Jyske Bank A/S' udgifter til advokat-bistand, er uden moms, da det er oplyst, at Jyske Bank A/S er momsregistreret.

THI KENDES FOR RET:

Jyske Bank A/S frifindes.

Sagsøger skal til Jyske Bank A/S betale sagsomkostninger med 50.000 kr.

Sagsomkostningerne skal betales inden 14 dage og forrentes efter rentelovens § 8 a.


DANMARKS DOMSTOLE