



ØSTRE LANDSRET DOM

afsagt den 2. oktober 2026

Sag BS-26876/2025-OLR
(10. afdeling)

A
(advokat Iben Gjessing, beskikket)

mod

Nordea Danmark, Filial af Nordea Bank Abp, Finland
(advokat Amelie Brofeldt)

Biintervenient:
Finans Danmark
(advokat Martin Dahl Pedersen)

Københavns Byret har den 7. maj 2025 afsagt dom i 1. instans (sag BS-28021/2023-KBH).

Landsdommerne Katja Høegh, Anne Bendfeldt Westergaard og Louise Hauberg Wilhelmsen har deltaget i ankesagens afgørelse.

Påstande

Appellanten, A, har nedlagt påstand i det væsentlige som for byretten om, at Nordea Danmark, filial af Nordea Bank Abp, Finland, tilpligtes til A at betale 398.957,62 kr. med procesrente fra den 5. september 2022, subsidiært et lavere beløb.

Indstævnte, Nordea Danmark, Filial af Nordea Bank Abp, Finland ("Nordea"), har påstået dommen stadfæstet.

Biintervenienten, Finans Danmark, har tilsluttet sig Nordeas påstand om stadfæstelse.

A har også for landsretten fri proces og retshjælpsdækning i Alka Forsikring (skadenr. 3769425-T01MEMI).

A har for landsretten frafaldet sine anbringender om ugyldighed efter aftalelovens § 28 og § 29, om at Nordea hæfter i medfør af vilkårene i parternes netbanksaftale, og om at Nordea havde en burde-viden efter reglerne i hvidvaskloven.

A har med landsrettens tilladelse efter retsplejelovens § 383, stk. 1, jf. stk. 2, in fine, fremsat et nyt anbringende om, at det er ansvarspådragende, at Nordea ikke straks sikrede tilbageførsel ved As henvendelse ved fysisk fremmøde om formiddagen den 23. august 2022 straks efter misbruget den foregående aften.

Supplerende sagsfremstilling

Der er for landsretten yderligere fremlagt Nationalbankens kvartalsoversigt, 3. kvartal 2014 af 23. september 2014, hvoraf fremgår bl.a.

”I november 2014 bliver det muligt for borgere og virksomheder i Danmark at overføre penge øjeblikkeligt, døgnet rundt alle årets dage, mod i dag, hvor der kan gå flere dage, før en betaling når frem til modtageren.

Muligheden for at foretage sådanne straksoverførsler er kulminationen på en modernisering af den danske betalingsinfrastruktur, som er gennemført i et samarbejde mellem den finansielle sektor og Nationalbanken med omtale af mulighed for straksoverførsler af pengebeløb i den danske banksektor fra november 2014.”

I fodnote 2 oplyses det:

”Det er mellem pengeinstitutterne aftalt, at en straksoverførsel maksimalt kan være på 500.000 kr. Det enkelte institut kan dog individuelt sætte en lavere beløbsgrænse.”

Af pengeinstitutternes generelle overførselsoverenskomst af 1. juli 2016 fremgår bl.a.:

”§ 1 Aftalens parter

Aftalen omfatter Pengeinstitutternes behandling af Kreditoverførsel foretaget gennem Intradagclearingen, Straksclearingen og Dokumentløs Clearing.

...

§ 5 Tilbagekaldelse

Datagrundlaget kan tilbagekaldes, inden beløbet er krediteret Betalingsmodtagers konto.

...

§ 6 Tilbageførsel ved Åbenlyse fejl

Overførte beløb, der er bogført på Betalingsmodtagers konto, kan som hovedregel ikke tilbageføres.

Tilbageførsel kan dog ske, hvis en overførsel efter Betalingsafsenders Pengeinstituts opfattelse er behæftet med Åbenlyse fejl....

...

§ 7 Tilbageførsel ved Fraud

Overførte beløb, der er bogført på Betalingsmodtagers konto, kan som hovedregel ikke tilbageføres.

Tilbageførsel kan dog ske, hvis en overførsel efter Betalingsafsenders Pengeinstituts opfattelse skal betragtes som økonomisk kriminalitet, se også "Vejledning til pengeinstitutter ved netbankmisbrug" (bilag 8 til Rammeaftalen) på Finans Danmark medlemsnet. Tilbageførsel foretages på anmodning fra Betalingsafsenders Pengeinstitut, og Betalingsafsenders Pengeinstitut friholder Betalingsmodtagers Pengeinstitut for enhver risiko og ethvert ansvar forbundet med tilbageførslen, herunder tab som opstår, hvor tilbageførslen resulterer i et overtræk som følge af, at Betalingsmodtager har nået at disponere over et beløb, som tilbageføres."

Der er i tillæg til det for byretten fremlagte fremlagt følgende yderligere rapporter og artikler med omtale af svindel i form af bedrageriske telefonopkald ("safe account fraud") svarende til, hvad A var udsat for:

- "Impersonation scams almost double in first half of 2020 as criminals exploit", artikel offentliggjort af UK Finance den 29. september 2020.
- "Internet Organised Crime Threat Assessment (IOCTA)", rapport offentliggjort den 11. november 2021 af Europol, hvoraf fremgår bl.a.:

"An emerging modus operandi in vishing is the safe account scam. In this type of fraud, criminals call their targets pretending to be employees of financial institutions or the police with spoofed caller IDs, informing them that they need to protect their money from criminals. To do so, they are instructed to transfer their funds to a 'safe account', which is under the control of the criminals and subsequently used in a network of money mules to launder the illicit proceeds. As with other vishing scams, the safe account scam often targets specific victims with the help of compromised information."

- "Ny svindel: Kunder bliver narret til at overføre deres penge", artikel offentliggjort på Lån & Spars hjemmeside den 11. februar 2022.
- "Pas på de kriminelle i telefonen – sidste år stjal netbanksvindlerne 96 mio. kroner", artikel offentliggjort af Finans Danmark den 5. maj 2023
- Nationalbankens analyse "Digital payment fraud in Denmark" af 29. april 2024.
- "Svindelsager mere end fordoblet på et år – men bankerne stopper over halvdelen", artikel offentliggjort af Finans Danmark den 11. april 2024.
- "Færre bliver net-banksvindlet – men de kriminelle slap stadig væk med over 80 mio. kroner sidste år", artikel offentliggjort af Finans Danmark den 3. marts 2025.

For landsretten er endvidere fremlagt skærmfotos fra Internet Archive Way-back Machine (archive.org) af Nordeas hjemmeside, som den fremstod i perioden 19. til 31. september 2021, og som viser, at Nordea i perioden på en underside om "Sådan undgår du at blive udsat for svindel", der var tilgængelig via et link "Undgå digital svindel" nederst på Nordeas hjemmeside, indeholdt advarsler, som lød:

"Lav aldrig en overførsel, fordi nogen forsøger at overtale dig til det over telefonen.

...

Læg på, hvis nogen over telefonen vil overtale dig til at lave en overførsel."

Af en oversigt over afgørelser fra Det Finansielle Ankenævn angående nævnets sager om bedrageriske telefonopkald i perioden 9. november 2021 til 31. oktober 2025 fremgår bl.a.:

AFGØRELSE TRUFFET AF DET FINANSIELLE ANKENÆVN - BEDRAGERISKE TELEFONOPKALD											
Nyt dok											
Afgørelsesdato	Journalnr.	Gerningstidspunktet	Til	Pengeinstitut	Beløb	Tab	Alder (år)	Køn	Dommerfordeling	Bemærkninger	
IFANSE	IFANSE	Fra	Til				Klager	Klager	Med klager	For klager	
9. november 2021	91/2021	28. oktober 2020	28. oktober 2020	Nordea Bank	165.000 kr.	165.000 kr.		K	AFVIST		
24. maj 2022	412/2021	11. september 2021	11. september 2021	Danske Bank	133.300 kr.	30.000 kr.	88	K	AFVIST		
4. juli 2022	455/2021	20. august 2021	23. august 2021	Nordea Bank	623.100 kr.	434.500 kr.	79	K	5	0	
4. juli 2022	395/2021	8. august 2021	8. august 2021	Nordea Bank	687.007 kr.	382.099 kr.		K	5	0	
20. september 2022	565/2021	6. november 2021	6. november 2021	Nordea Bank	249.000 kr.	238.848 kr.		K	5	0	
20. oktober 2022	589/2021	18. november 2021	18. november	Spar Nord Bank	72.744 kr.	29.900 kr.	76	K	3	2	Dissens
20. oktober 2022	58/2022	7. oktober 2021	7. oktober 2021	Nordea Bank	84.900 kr.	34.900 kr.		K	3	2	Dissens
20. oktober 2022	525/2021	4. september 2021	15. september 2021	Nordea Bank	ca. 67.900 kr.	54.944 kr.		K	3	2	Dissens
20. oktober 2022	39/2022	18. september 2021	18. september 2021	Danske Bank m.fl.	163.000 kr.	142.534 kr.		K	3	2	Dissens
2. november 2022	91/2022	29. november 2021	29. november 2021	Lån & Spar Bank	30.000 kr.	17.778 kr.		K	3	2	Dissens
12. december 2022	128/2022	16. november 2021	16. november 2021	Nordea Bank	-	-		K	3	2	Dissens
18. januar 2023	126/2022	5. januar 2022	6. januar 2022	Nordea Bank	564.000 kr.	416.648 kr.	76	K	3	2	Dissens
15. februar 2023	003/2022	16. oktober 2021	16. oktober 2021	Middelfart Sparekasse	19.300 kr.	19.300 kr.		M	AFVIST		
21. marts 2023	271/2022	28. juni 2022	28. juni 2022	Nordea Bank	96.000 kr.	96.000 kr.		M/K	3	2	Dissens

Af oversigten fremgår tillige følgende om fordeling mellem forskellige banker af denne type klagesager:

Antal afgørelser pr. bank:		
Bank	Medvirken i afgørelser	% af samlede sager
Nordea	69	52,67%
Øvrige	19	14,50%
Danske Bank	17	12,98%
Nykredit	13	9,92%
Lån & Spar	9	6,87%
Jyske Bank	6	4,58%
Sydbank	3	2,29%
Afgørelser i alt	131	

I et eksempel (udateret) på en SMS-besked afgivet af den svenske bank SEB ses følgende advarsel:

”Kom ihåg! Vi på SEB kommer aldrig ringa för att be dig skriva under något. Har du blivit uppringd? Avbryt signeringen och avsluta genast samtalet och kontakta oss på SEB själv.”

Af sagsfremstillingen i Det Finansielle Ankenævns afgørelse af 31. maj 2024 i sag 665/2023 angående Nordeas påståede hæftelse i en sag om telefonisk bedrageri, som det her foreliggende, fremgår:

”Banken har endvidere oplyst, at der som en ekstra sikkerhed ved overførslen blev sendt en SMS til klagerens telefonnummer, hvortil der skulle svares ”JA”, hvis overførslen skulle gennemføres. Banken har fremlagt en SMS-log, hvoraf det fremgår, at der inden overførslen blev sendt SMS med følgende tekst til klagerens telefonnummer:

”OBS! Hvis en anden har bedt dig overføre penge, kan det være svindel. I tvivl? Ring til os via din mobilbank-app eller på 70 33 11 01. Bekræft overførsel af 90.123,00 kr. til konto
Svar JA, hvis den skal gennemføres - NEJ, hvis den ikke skal gennemføres. Venlig hilsen Nordea”

I anledning af As nye anbringende for landsretten om tilbageførsler har Nordea ved en mail af 15. september 2026 fra Lead Fraud Investigator i Nordea, Daoud Reda, sammenfattet regnskabet på de tre konti i Nordea, hvortil A foretog overførsler, som følger:

”Vedr. modtagerkonto 5501-9024759528 som modtager samlet 200.764,00 kr

22.08.2022 kl. 21:22 PENGEAUTOMAT	5.000,00 kr.
22.08.2022 kl. 21:43 fra konto 5501-9024759528 til konto 6695-1000821248	49.000,00 kr
22.08.2022 kl. 23:52 fra konto 5501-9024759528 til konto 6695-1000821248	75.000,00 kr.

23.08.2022 ukendt tidspunkt udenlandsk overførsel 13.900,00 kr.
 23.08.2022 kl. 00:55 9024759528 00009028784705 5.000,00 kr
 kundens egen grundkonto (midlerne bliver sendt til udlandet)

Nuværende saldo: 53.133,55 kr
 Reservationer på kortet: 53.115,81 kr

Der bliver også brugt andre små beløb forskellige steder på kortet, men der er desværre ingen midler sikre på kontoen.

BEMÆRK: Vi har desværre ingen timestamp på den udenlandske overførsel, men transaktionen er formentlig foretaget i forbindelse med at kunden også foretager den interne transaktion mellem egne konti.

Vedr. modtagerkonto 9163-6888933334 som modtager 53.981,00 kr

22.08.2022 kl. 21:59 fra konto 9163-6888933334	
til konto 9236-4568373834	15.000,00 kr
22.08.2022 MOBILEPAY OVERFØRSEL	5.000,00 kr
23.08.2022 NORDEA PAY KØB	48,00 kr
23.08.2022 NORDEA PAY KØB	48,00 kr
23.08.2022 NORDEA PAY KØB	27,00 kr
23.08.2022 NORDEAPAY UDB.	100,00 kr
23.08.2022 kl. 01:00 fra konto 9163-6888933334	
til konto 5295-0012001509	16.994,00 kr

Reservationer på kortet: 17.000 kr.
 Nuværende saldo: 17.000 kr.

Ingen midler sikret.

Vedr. modtagerkonto 2277-6291843296 som modtager 60.740,00 kr

Kunden flytter pengene mellem sine konti og tilbage til konto 6291843296

22.08.2022 kl. 22:12 fra konto 6291843296	
til konto 00008977704333	5.000,00 kr
22.08.2022 kl. 22:20 fra konto 6291843296	
til konto 00008977704333	12.140,02 kr
22.08.2022 kl. 23:14 fra konto 6291843296	
til konto 00008977704333	10.040,02 kr
23.08.2022 kl. 00:11 fra konto 6291843296	
til konto 00008977704333	10.040,02 kr

UD fra konto 6291843296	
22.08.2022 kl. 20:56 PENGEAUTOMAT	3.000,00 kr
22.08.2022 kl. 22:21 PENGEAUTOMAT	5.000,00 kr
22.08.2022 ukendt tidspunkt MOBILEPAY	10.000,00 kr
23.08.2022 ukendt tidspunkt MOBILEPAY	9.900,00 kr
23.08.2022 ukendt tidspunkt MOBILEPAY	40,02 kr

Nuværende saldo på begge konti: 30.699,98 kr
 Reservationer på kortet samlet: 32.599,98 kr.

Ingen midler sikret.”

Parterne er enige om, at det anførte er i overensstemmelse med, hvad der fremgår af det underliggende materiale.

Retsgrundlaget

Lov om finansiel virksomhed

Det fremgår af lov om finansiel virksomhed §§ 43 og 43 a:

”§ 43. Finansielle virksomheder og finansielle holdingvirksomheder skal drives i overensstemmelse med redelig forretningsskik og god praksis inden for virksomhedsområdet.

Stk. 2. Erhvervsministeren fastsætter nærmere regler om redelig forretningsskik og god praksis for de finansielle virksomheder. Erhvervsministeren fastsætter, jf. 1. pkt., regler om indholdet af en basal indlånskonto og om størrelsen af et eventuelt gebyr for en sådan konto.

...

§ 43 a. Handlinger i strid med regler udstedt i medfør af § 43, stk. 2, pådrager erstatningsansvar i overensstemmelse med dansk rets almindelige regler.”

Erhvervsministeren har i medfør af lovens § 43, stk. 2, udstedt bekendtgørelse nr. 330 af 7. april 2016 om god skik for finansielle virksomheder med senere ændringer. Af bekendtgørelsen følger bl.a.:

”§ 3. En finansiel virksomhed skal handle redeligt og loyalt over for sine kunder, jf. dog stk. 2

...

§ 8. Ved rådgivning forstås anbefalinger, vejledninger, herunder oplysninger om risici forbundet med en disposition, og oplysninger om umiddelbare konsekvenser af kundens valgmuligheder.

Stk. 2. En finansiel virksomhed skal yde rådgivning, hvis kunden anmoder herom, jf. dog § 2. Endvidere skal virksomheden af egen drift yde rådgivning, jf. dog stk. 5, hvor omstændighederne tilsiger, at der er behov herfor.

Stk. 3. Rådgivningen skal tilgodese kundens interesser og give kunden et godt grundlag for at træffe sin beslutning. Rådgivningen skal være relevant, retvisende og fyldestgørende. Den finansielle virksomhed skal orientere om de risici, der er relevante for kunden.”

I vejledning nr. 9971 af 23. september 2016 til bekendtgørelsen om god skik for finansielle virksomheder er det anført bl.a.:

”Kapitel 4. Rådgivning

§§ 8-10 er en udmøntning af »kend din kunde-princippet«. Princippet er her udstrakt til at gælde alle typer finansiel virksomhed, og det forudsætter, at den finansielle virksomhed foretager en undersøgelse af kundens forhold forud for, at der ydes rådgivning, således

at rådgivningen kan tage udgangspunkt i kundens individuelle forhold.

...

Der er ikke pligt til at rådgive, hvis kunden alene efterspørger en »ren« ekspedition, jf. dog § 2. Som eksempler på »rene« ekspeditioner kan nævnes ind- og udbetalinger, pengeoverførsler og valutaveksling. Der skal dog rådgives, hvis »omstændighederne tilsiger, at der er behov herfor«. Det kan f.eks. være, når kunden har behov for rådgivning under en ekspedition eller i andre tilfælde, hvor rådgivningsbehovet viser sig ved anden kontakt med den finansielle virksomhed. Der vil endvidere altid være behov for rådgivning i forbindelse med optagelse af lån i fremmed valuta på grund af risikoen for valutakursudsving. Dette gælder dog ikke større virksomheder, som har den fornødne indsigt til at kunne forstå de risici, der er forbundet med at optage lån i fremmed valuta.”

Betalingsloven

Det følger af den nugældende betalingslov fra 2017 (lov nr. 652 af 8. juni 2017 med senere ændringer) bl.a.:

”§ 82. En betalingstransaktion er kun autoriseret, hvis betaleren har meddelt samtykke til at gennemføre transaktionen. Betaleren kan autorisere betalingstransaktionen før eller efter gennemførelsen af denne, hvis det er aftalt mellem betaleren og dennes udbyder. Er der ikke meddelt samtykke, skal betalingstransaktionen anses for uautoriseret.

Stk. 2. Samtykke meddeles i den form, der er aftalt mellem betaleren og dennes udbyder. Det kan herunder aftales, at samtykke til at gennemføre en betalingstransaktion tillige kan gives via betalingsmodtageren eller en udbyder af betalingsinitieringstjenester.

Stk. 3. Betaleren kan tilbagekalde et samtykke efter stk. 1 indtil det tidspunkt, der følger af § 111. Et samtykke til at gennemføre en række betalingstransaktioner kan også tilbagekaldes, hvorefter eventuelle fremtidige betalingstransaktioner skal anses for uautoriserede.

...

§ 99. Betalerens udbyder af betalingstjenester hæfter i forhold til betaleren for tab som følge af uautoriserede betalingstransaktioner, jf. § 97, medmindre andet følger af § 100. Ved en uautoriseret transaktion skal betalerens udbyder straks og senest ved afslutningen på den efterfølgende arbejdsdag tilbagebetale betaleren beløbet, medmindre betalerens udbyder har rimelige grunde til at have mistanke om svig og underretter Finanstilsynet om disse grunde.

Stk. 2. Hvor en uautoriseret betalingstransaktion er iværksat via en udbyder af betalingsinitieringstjenester, skal den kontoførende udbyder tilbagebetale betaleren beløbet straks og senest ved afslutningen på den efterfølgende arbejdsdag, jf. stk. 1.

Stk. 3. Er udbyderen af betalingsinitieringstjenester ansvarlig for den uautoriserede betalingstransaktion, skal udbyderen af betalingsinitieringstjenesten efter den kontoførende udbyders anmodning straks holde den kontoførende udbyder skadesløs for tab eller betalte beløb som følge af tilbagebetalingen til betaleren, jf. § 98, stk. 3.

Stk. 4. Finanstilsynet fastsætter nærmere regler om den tekniske gennemførelse af underretningen, jf. stk. 1, 2. pkt.

§ 100. Betalerens udbyder af betalingstjenester hæfter i forhold til betaleren for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af stk. 2-5. Betaleren hæfter kun efter stk. 3-5, hvis transaktionen er korrekt registreret og bogført, jf. dog stk. 2.

Stk. 2. Betaleren hæfter uden beløbsbegrænsning for tab, der opstår, som følge af at betaleren har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter § 93.

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

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

- 1) at betaleren har undladt at underrette betalerens udbyder snarest muligt efter at have fået kendskab til, at det til betalingstjenesten hørende betalingsinstrument er bortkommet eller den personlige sikkerhedsforanstaltning er kommet til den uberettigedes kendskab,
- 2) at betaleren med forsæt har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 5, eller
- 3) at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

Stk. 5. Betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt og betalerens udbyder godtgør, at betaleren med forsæt har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug.

...

§ 109. En betalingsordre anses for modtaget på det tidspunkt, hvor betalingsordren modtages af betalerens udbyder. Betalerens konto må ikke debiteres før dette tidspunkt. Hvis tidspunktet for modtagelsen ikke er en arbejdsdag, anses betalingsordren for at være modtaget den følgende arbejdsdag.

Stk. 2. En udbyder kan bestemme, at en betalingsordre, som er modtaget tæt på slutningen af en arbejdsdag, skal anses for at være modtaget den følgende arbejdsdag.

Stk. 3. Aftaler brugeren med udbyderen, at betalingsordren først skal gennemføres på et senere tidspunkt, anses betalingsordren for modtaget på den aftalte dato, hvis dette er en arbejdsdag, og ellers på den førstkommande arbejdsdag derefter.

...

§ 111. En betalingsordre kan ikke tilbagekaldes, efter at den er modtaget af betalerens udbyder, jf. § 109, jf. dog stk. 2-5.

Stk. 2. En betalingsordre iværksat af en udbyder af betalingsinitieringstjenester eller af eller via betalingsmodtageren kan ikke tilbagekaldes, efter at betaleren har afgivet sit samtykke til at gennemføre betalingstransaktionen til udbyderen af betalingsinitieringstjenesten eller betalingsmodtageren.

Stk. 3. En betalingsordre i forbindelse med direkte debitering kan tilbagekaldes senest ved slutningen af arbejdsdagen før den aftalte dato for debitering af midlerne.

Stk. 4. En betalingsordre omfattet af § 109, stk. 3, kan tilbagekaldes senest ved slutningen af arbejdsdagen før den aftalte dato.

...

§ 128. En udbyder af betalingstjenester skal anvende stærk kundeautentifikation, medmindre andet følger af forordninger og regler udstedt af Kommissionen i medfør af artikel 98 i Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked, når en bruger

- 1) tilgår sin betalingskonto online,
- 2) iværksætter en elektronisk betalingstransaktion eller
- 3) udfører handlinger gennem en enhed til fjernkommunikation, der kan indebære risiko for misbrug.

Stk. 2. Ved iværksættelse af elektroniske betalinger, jf. stk. 1, nr. 2, via en enhed til fjernkommunikation skal udbyderen sikre, at der anvendes stærk kundeautentifikation, som omfatter elementer, der dynamisk knytter transaktionen til et specifikt beløb og en specifik betalingsmodtager.

Stk. 3. Ved iværksættelse af betalingstransaktioner via en betalingsinitieringstjeneste, jf. bilag 1, nr. 7, finder stk. 2 også anvendelse.

Stk. 4.

Når en udbyder af kontooplysningstjenester anmoder om data til brug for udbuddet af tjenester omfattet af bilag 1, nr. 8, finder stk. 1 også anvendelse.

Stk. 5. Den kontoførende udbyder skal give udbydere af betalingsinitieringstjenester og kontooplysningstjenester tilladelse til at anvende de autentifikationsprocedurer, som den kontoførende udbyder stiller til rådighed for dennes brugere, jf. stk. 1 og 2."

I forarbejderne hertil i lovforslag nr. L 157 af 15. marts 2017 er det anført bl.a.:

"Almindelige bemærkninger

1. Indledning

Lovforslaget erstatter den gældende lov om betalingstjenester og elektroniske penge (lovbekendtgørelse nr. 613 af 24. april 2015) og gennemfører Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked (herefter 2. betalingstjenestedirektiv) i dansk ret.

...

Den nugældende lov om betalingstjenester og elektroniske penge

blev vedtaget i 2009. Siden da er der sket store teknologiske fremskridt på it-området, som har gjort det muligt at udvikle nye online og mobile betalingsløsninger, som der ikke var tænkt på under tilblivelse af den nugældende lov. Mange nye betalingstjenester falder derfor slet ikke, eller kun i mindre grad, ind under anvendelsesområdet for den nugældende lov. Som følge af udviklingen på området har der været et behov for at håndtere nye sikkerhedsrisici og en manglende forbrugerbeskyttelse på visse områder.

Lovforslagets hovedformål er at sikre, at rammerne for udbuddet af elektroniske betalingstjenester fortsat er tidssvarende og reflekterer den teknologiske udvikling. Med lovforslaget fastsættes nye regler, der vil give en klarere retsstilling og sikre ensartede vilkår for alle udbydere af betalingstjenester. Det indebærer blandt andet, at såkaldte tredjepartsudbydere, dvs. udbydere af betalingstjenester, som er en anden end den udbyder af betalingstjenester, hos hvem en bruger har sin konto, også bliver omfattet af lovforslaget. Hermed bliver disse tredjepartsudbyderes retsstilling klarlagt, og der sikres ligeledes en passende forbrugerbeskyttelse i relation til disses aktiviteter. Klare regler for disse udbydere vil også sikre en bedre konkurrence på markedet for betalinger til glæde for primært forbrugerne og detailhandlen.

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

...

8. Forholdet til EU-retten

...

Lovforslaget er som udgangspunkt udtryk for direktivnær gennemførelse, men på en række områder er det dog vurderingen, at loven fortsat bør gå videre end direktivets krav for at kunne sikre en tilstrækkelig forbrugerbeskyttelse og en bibeholdes af eksisterende danske løsninger, særligt vedrørende Dankortet.

...

2. betalingstjenestedirektiv artikel 74 giver medlemslandene mulighed for at fastsætte hæftelsesregler, der stiller forbrugeren bedre end direktivs krav. Denne mulighed er anvendt til i tilfælde, hvor forbrugeren undlader at underrette udsteder af betalingsinstrumentet om, at det er stjålet, eller forbrugeren optræder groft uforsvarligt at fastsætte en hæftelsesgrænse for forbrugeren på op til 8.000 kr. Direktivet fastsætter i dette tilfælde en ubegrænset hæftelse for forbrugeren. De eksisterende danske regler, der har været anvendt siden 1999, er forankret i gældende praksis på området, som det ikke anses for hensigtsmæssigt at ændre.

§§ 102-106, i gældende lov om betalingstjenester og elektroniske penge fastsætter regler for de såkaldte betalingssurrogater, som omfatter elektroniske systemer, i det omfang de kan benyttes til at

erhverve varer eller tjenesteydelser, uden at det udgør en betalingstjeneste. Derudover reguleres udbydere af betalingsinstrumenter med begrænset anvendelse, eksempelvis benzinkort eller rejsekort, jf. gældende lovs § 37, stk. 1, nr. 1. Disse typer af tjenester er ikke omfattet af 2. betalingstjenestedirektiv. Men henblik på at reducere de erhvervsøkonomiske byrder ophæves disse bestemmelser med dette lovforslag, således at disse virksomheder der udbyder betalings-surrogater ikke længere skal registreres ved Forbrugerombudsmanden og virksomheder, der udsteder betalingsinstrumenter med begrænset anvendelse ikke længere skal opnå tilladelse ved Finanstilsynet. Med henblik på stadig at sikre forbrugerne en passende beskyttelse foreslås det dog, at disse tjenester fortsat skal være omfattet af visse af lovforslagets forbrugerbeskyttende regler. Dette fastsættes i lovforslagets § 1, stk. 5, og § 5, nr. 14-16. Idet dette lovforslag indeholder en række danske særregler der går udover de fælles europæisk regler på området foreslås det i § 1, stk. 7, at erhvervsministeren kan dispensere helt eller delvist fra lovens danske særregler, således at det i tilfælde, hvor det vil forekomme urimeligt byrdefuldt at lade lovens danske særregler finde anvendelse eller hvor der er andre samfundsmæssige hensyn, der gør sig gældende. Denne mulighed skal dog anvendes restriktivt.

...

Bemærkninger til lovforslagets enkelte bestemmelser

...

Til § 82

Det følger af § 57, i den nugældende lov om betalingstjenester og elektroniske penge, at en betalingstransaktion kun er autoriseret, hvis betaleren har meddelt samtykke. Samtykket skal meddeles i den form der er aftalt, og kan ikke tilbagekaldes efter det tidspunkt, der er anført i lovens § 73.

Den foreslåede bestemmelse i § 82 viderefører med indholdsmæssige ændringer § 57, i den nugældende lov om betalingstjenester og elektroniske penge og gennemfører samtidig 2. betalingstjenestedirektiv artikel 64.

Det foreslås i *stk. 1*, at en betalingstransaktion kun er autoriseret, hvis betaleren har meddelt samtykke til at gennemføre transaktionen. Betaleren kan autorisere betalingstransaktionen før eller efter gennemførelsen af denne, hvis det er aftalt mellem betaleren og dennes udbyder. Er der ikke meddelt samtykke, skal betalingstransaktionen anses for uautoriseret.

Med autorisere forstås at godkende. Begrebet autorisering anvendes i praksis ved gennemførelse af betalingstransaktioner. Som eksempler på betalers meddelelse af samtykke kan nævnes, at betaler anvender sin pinkode i en forretning, underskriver en betalingsordre i en filial eller anvender sin kode i en netbank.

Det er en forudsætning for, at en betalingstransaktion kan autoriseres efter gennemførelsen af betalingstransaktionen, at der forinden er indgået en specifik aftale herom mellem betaleren og udbyderen. Det beror på en konkret vurdering, hvorvidt der i det enkelte tilfælde er indgået en sådan aftale.

Det foreslås i *stk. 2*, at samtykke meddeles i den form, der er aftalt

mellem betaleren og dennes udbyder. Det kan herunder aftales, at samtykke til at gennemføre en betalingstransaktion tillige kan gives via betalingsmodtageren eller en udbyder, der udbyder betalingsinitieringstjenester.

Bestemmelsen fastsætter ikke krav til, hvordan et samtykke skal meddeles. Det beror på den aftale der er indgået mellem parterne, hvordan betaler konkret skal meddele sit samtykke. Betalers udbyder skal oplyse om dette i rammeaftalen, jf. lovforslagets § 72, stk. 1, nr. 2, litra c.

Betaler skal meddele samtykket til dennes udbyder, men lovforslaget stiller ikke nogen krav om, hvordan samtykket meddeles.

Betaler kan således give samtykket direkte til sin udbyder, eksempelvis ved at give samtykke til en kontooverførsel via netbank ved anvendelse af en kode, eller betaler kan give det indirekte til sin udbyder via betalingsmodtageren, eksempelvis ved en kortbetaling, hvor betaler giver sit samtykke ved at indtaste sin PIN-kode eller ved at samtykket gives via en udbyder, der udbyder betalingsinitieringstjenester, som videreformidler det til den kontoførende udbyder. Det foreslås i *stk. 3*, at betaleren kan tilbagekalde et samtykke efter *stk. 1* indtil det tidspunkt, der følger af § 111. Et samtykke til at gennemføre en række betalingstransaktioner kan også tilbagekaldes, hvorefter eventuelle fremtidige betalingstransaktioner skal anses for uautoriserede.

Betaler kan indtil tidspunktet fastsat i lovforslagets § 111 tilbagekalde et samtykke. En betalingsordre kan som udgangspunkt ikke tilbagekaldes efter, at den er modtaget af betalers udbyder. Der gælder dog undtagelser for betalingsordre, hvor samtykket er meddelt via betalingsmodtager eller en udbyder, der udbyder betalingsinitieringstjenester, jf. nærmere herom i bemærkningerne til lovforslagets § 111, hvortil der henvises.

...

Lovforslagets bestemmelser vedrører alene betalers tilbagekaldelse af samtykke over for dennes udbyder, idet lovforslaget kun regulerer forholdet mellem betaler og denne udbyder, og ikke den eventuel underliggende aftale mellem betaler og betalingsmodtager. Lovforslaget berører således ikke, at forbrugeren altid vil kunne henvende sig til betalingsmodtageren, hvis forbrugeren ikke mener, at der er indgået en aftale, og meddele betalingsmodtageren, at der ikke må trækkes penge på forbrugers konto.

...

Til § 99

Det følger af § 61 i den nugældende lov om betalingstjenester og elektroniske penge, at betalers udbyder hæfter i forhold til betaler for tab som følge af uautoriserede betalingstransaktioner, jf. § 57, medmindre andet følger af § 62. Ved en uautoriseret transaktion skal betalers udbyder straks tilbagebetale betaleren beløbet. Den foreslåede bestemmelse i § 99 viderefører med visse indholdsmæssige ændringer § 61 i lov om betalingstjenester og elektroniske penge. Bestemmelsen gennemfører 2. betalingstjenestedirektiv artikel 73.

Det foreslås i *stk. 1*, at betalers udbyder hæfter i forhold til betaler

for tab som følge af uautoriserede betalingstransaktioner, jf. § 97, medmindre andet følger af § 100. Ved en uautoriseret transaktion skal betalers udbyder straks, og senest ved afslutningen på den efterfølgende arbejdsdag, tilbagebetale betaleren beløbet, medmindre betalerens udbyder har rimelige grunde til at have mistanke om svig og underretter Finanstilsynet om disse grunde.

...

Hvorvidt der er tale om en uautoriseret betalingstransaktion skal vurderes efter lovforslagets § 82, som fastsætter regler om samtykke til betalingstransaktioner.

Udbyderen kan undlade at tilbagebetale beløbet til betaleren straks, hvis udbyderen har rimelig grund til at mistænke betaleren for at handlet svigagtige, under forudsætning af at udbyderen underretter Finanstilsynet om disse grunde. Formålet med dette er dels, at Finanstilsynet generelt får mulighed for at overvåge misbrugsbilledet for betalinger i Danmark samt dels, at Finanstilsynet får mulighed for at føre tilsyn med at enkelte udbydere ikke systematisk uretmæssigt forhindrer brugerne i at få tilbagebetalt de midler, de har ret til ifølge lovforslaget. Det er således ikke hensigten, at Finanstilsynet skal behandle de enkelte sager, da disse behandles af det relevante ankenævn.

Udbyderen kan kun tilbageholde beløbet indtil mistanken om svig er bekræftet eller afkræftet. Bestemmelsen skal ses som en undtagelse til hovedreglen om at tilbagebetale beløbet straks, og skal kun anvendes i særlige tilfælde. Der skal derfor altid foretages en konkret vurdering, hvorfor bestemmelsen ikke kan anvendes som en generel regel i forbindelse med en betalers indsigelse mod en uautoriseret autentifikation. Retten til at holde beløbet tilbage ophører i det øjeblik, hvor mistanken om svig ikke længere kan siges at være berettiget.

...

Til § 100

Det følger af § 62 i den nugældende lov om betalingstjenester og elektroniske penge, at betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af et betalingsinstrument, medmindre andet følger af stk. 2-6. Betaler hæfter kun efter stk. 2-6, hvis transaktionen er korrekt registreret og bogført. Ved en uberettiget anvendelse af et betalingsinstrument skal betalers udbyder straks tilbagebetale betaleren beløbet. Betaleren hæfter dog uden beløbsbegrænsning for tab, der opstår som følge af, at betaler har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter § 59.

Forslaget til § 100 fastlægger den ansvarsfordeling, som skal gælde, hvis et betalingsinstrument bruges af en person, som ikke er berettiget til at bruge det.

Den foreslåede bestemmelse viderefører med visse indholdsmæssige ændringer § 62 i den nugældende lov om betalingstjenester og elektroniske penge. Bestemmelsen gennemfører artikel 74, i 2. betalingstjenestedirektiv. Idet det dog følger af artikel 74, 4. pkt., i 2. betalingstjenestedirektiv, at medlemslandene kan fastsætte andre hæftelses- og ansvarsregler for betaleren, hvis denne hverken har

optrådt svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser i henhold til artikel 69 i 2. betalingstjenestedirektiv, der er gennemført i dette lovforslags § 93.

Der er således hensigten med forslaget til § 100 at videreføre eksisterende praksis vedrørende hæftelses- og ansvarsreglerne i forbindelse med uberettigede anvendelse af en betalingstjeneste, dog med de to ændringer, der følger af 2. betalingstjenestedirektiv. Med disse to ændringer indføres to nye ansvarsnormer, idet betaler ifølge 2. betalingstjenestedirektiv ikke hæfter for tab, såfremt betalernes udbyder ikke kræver stærk kundeautentifikation, medmindre betaleren har handlet svigagtigt, eller hvis betaler ikke med rimelighed kunne opdage tabet, tyveriet eller den uberettigede tilegnelse af det til betalingstjenesten hørende betalingsinstrument eller personlige sikkerhedsforanstaltning forud for den uberettigede anvendelse. Det foreslås i *stk. 1, 1. pkt.*, at betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af *stk. 2-5*.

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

Det følger af lovforslagets § 99, at betalers udbyder straks skal tilbagebetale beløbet for den uberettigede anvendelse af betalingsinstrumentet til betaleren. Dette indebærer, at betalers udbyder i tilfælde af en uautoriseret transaktion straks skal tilbagebetale betaleren beløbet. En udbyder bør derfor som udgangspunkt hurtigst muligt efter en anmeldelse om en uautoriseret transaktion tilbageføre det omtvistede beløb, og senest ved afslutningen på den efterfølgende arbejdsdag. Hvorvidt der er tale om en uautoriseret betalingstransaktion skal vurderes efter forslaget til § 82, som fastsætter regler om samtykke til betalingstransaktioner.

...

Det foreslås i *stk. 3*, at medmindre videregående hæftelse følger af *stk. 4 og 5*, hæfter betaleren med op til 375 kr. for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, hvis den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt.

Selvriskoreglen finder anvendelse i de tilfælde, hvor den til betalings-tjenesten hørende personlige sikkerhedsforanstaltning har været anvendt. Ved en personlig sikkerhedsforanstaltning forstås i overensstemmelse med § 7, nr. 31, personaliserede elementer, som udbyderen stiller til rådighed for brugeren med henblik på at foretage autentifikation. Det kan være en pinkode, men der er også andre personlige sikkerhedsforanstaltninger som for eksempel fingeraftryk og en enhed eller applikation til generering af engangskoder. Der er med definitionen således tiltænkt en teknologineutral definition, som skal tage højde for den teknologiske udvikling.

...

Det forudsættes som hidtil, at selvriskoen ikke vil blive gjort gældende af en udbyder over for en betaler i situationer, hvor det vil være klart stødende at lade betaleren hæfte, eksempelvis når

betalingssinstrumentet og koden er fratvunget betaleren ved anvendelse af vold, trussel om vold eller anden form for afpresning.

...

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

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

...

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

Det foreslås i *stk. 5*, at betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt og betalers udbyder godtgør, at betaleren med forsæt har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug.

...

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

Bestemmelsen understreger, at betaleren selv hæfter for tab, der opstår ved, at betaleren ved groft uforsvarlig adfærd eller bedrageri har muliggjort den uberettigede anvendelse. Det er dog en forudsætning, at betaler med forsæt har oplyst den personlige

sikkerhedsforanstaltning, der anvendes til at foretage stærk kundeautentifikation. I tilfælde, hvor betaler uforvarende har overladt den personlige

sikkerhedsforanstaltning til andre, eksempelvis i forbindelse med phishing, hæfter betaler ikke efter forslaget til stk. 5, idet betaler ikke overdrog den personlige sikkerhedsforanstaltning med forsæt på at der skal foretages den uberettigede anvendelse.

...

Det foreslås i *stk. 6*, at uanset *stk. 3-5* hæfter betalers udbyder for uberettiget anvendelse, der finder sted, efter at udbyderen har fået underretning om, at betalingsinstrumentet er bortkommet, at en uberettiget person har fået kendskab til den personlige sikkerhedsforanstaltning, eller at betaleren af andre grunde ønsker betalingsinstrumentet spærret, eller når det er forårsaget af handlinger, der er foretaget af en udbyders ansatte, agent eller filial eller en enhed, hvortil dens aktiviteter er outsourcet, eller disses passivitet, eller hvis udbyderen ikke har truffet egnede foranstaltninger, jf. forslagets § 94, stk. 1, nr. 2.

Bestemmelsen fastslår, at reglerne om betalers hæftelse i *stk. 3-5* fraviges i de tilfælde, hvor betalerens udbyder har handlet uagtsom ved at undlade at reagere på underretning, jf. denne bestemmelses nr. 1 og nr. 3.

...

Med forslaget til *stk. 8*, indføres en ny ansvarsnorm, idet betaler ikke ifalder ansvar, hvis betaler ikke med rimelighed havde mulighed for at opdage tabet, tyveriet eller den uberettigede tilegnelse af det til betalingstjenesten hørende betalingsinstrument eller personlige sikkerhedsforanstaltning forud for den uberettigede anvendelse. Forslaget gennemfører artikel 74, stk. 1, litra a, i 2. betalingstjenestedirektiv."

Den tidligere gældende lov nr. 385 af 25. maj 2009 om betalingstjenester indeholdt bl.a. følgende bestemmelser:

"§ 57. En betalingstransaktion er kun autoriseret, hvis betaleren har meddelt samtykke til at gennemføre betalingstransaktionen. Betaleren kan autorisere en betalingstransaktion før eller, hvis det er aftalt mellem betaleren og dennes udbyder, efter gennemførelsen af betalingstransaktionen.

Stk. 2. Et samtykke meddeles i den form og efter den procedure, der er aftalt mellem betaleren og dennes udbyder.

Stk. 3. Et samtykke kan ikke tilbagekaldes efter det tidspunkt, der følger af § 73.

...

§ 61. Betalers udbyder hæfter i forhold til betaler for tab som følge af uautoriserede betalingstransaktioner, jf. § 57, medmindre andet følger af § 62. Ved en uautoriseret transaktion skal betalers udbyder straks tilbagebetale betaleren beløbet.

Stk. 2. Det kan aftales, at stk. 1 ikke finder anvendelse ved mikrobetalingsinstrumenter, der anvendes anonymt, eller hvis betalers udbyder på grund af mikrobetalingsinstrumentets karakter ikke er i stand til at bevise, at betalingstransaktionen var autoriseret.

§ 62. Betalers udbyder hæfter i forhold til betaler for tab som følge af andres uberettigede anvendelse af et betalingsinstrument, medmindre andet følger af stk. 2-6. Betaler hæfter kun efter stk. 2-6, hvis transaktionen er korrekt registreret og bogført. Ved en uberettiget anvendelse af et betalingsinstrument skal betalers udbyder straks tilbagebetale betaleren beløbet. Betaleren hæfter dog uden beløbsbegrænsning for tab, der opstår som følge af, at betaler har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter § 59.

Stk. 2. Medmindre videregående hæftelse følger af stk. 3 eller 6, hæfter betaleren med op til 1.100 kr. for tab som følge af andres uberettigede anvendelse af betalingsinstrumentet, hvis den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning er anvendt.

Stk. 3. Medmindre videregående hæftelse følger af stk. 6, hæfter betaleren med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingsinstrumentet, hvis betalers udbyder godtgør, at den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning er anvendt, og

- 1) at betaleren har undladt at underrette betalers udbyder snarest muligt efter at have fået kendskab til, at betalingsinstrumentet er bortkommet, eller at den personlige sikkerhedsforanstaltning er kommet til den uberettigedes kendskab,
- 2) at betaleren har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 6, eller
- 3) at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

Stk. 4. Betaleren hæfter med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingsinstrumentet, når betalingsinstrumentet har været aflæst fysisk eller elektronisk, og den uberettigede i tilknytning hertil har anvendt en falsk underskrift og betalers udbyder godtgør,

- 1) at betaleren eller nogen, som betaleren har overladt betalingsinstrumentet til, har undladt at underrette betalers udbyder snarest muligt efter at have fået kendskab til, at betalingsinstrumentet er bortkommet, eller
- 2) at betaleren eller nogen, som betaleren har overladt betalingsinstrumentet til, ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

Stk. 5. Såfremt betaleren hæfter efter stk. 3 og 4, kan betalerens samlede hæftelse ikke overstige 8.000 kr.

Stk. 6. Betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingsinstrumentet, når den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning er anvendt og betalers udbyder godtgør, at betaleren har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug.

Stk. 7. Uanset stk. 2-6 hæfter betalers udbyder for uberettiget anvendelse, der finder sted, efter at udbyderen har fået underretning om, at betalingsinstrumentet er bortkommet, at en uberettiget person har fået kendskab til den personlige sikkerhedsforanstaltning, eller at betaleren af andre grunde ønsker betalingsinstrumentet spærret.

Stk. 8. Uanset stk. 2-6 hæfter betalers udbyder for uberettiget anvendelse, hvis udbyderen ikke har truffet egnede foranstaltninger, jf. § 60, stk. 1, nr. 2.

Stk. 9. Uanset stk. 2-6 hæfter betalers udbyder tillige, hvis betalingsmodtager vidste eller burde vide, at der forelå en uberettiget anvendelse af betalingsinstrumentet.

Stk. 10. Det kan aftales, at stk. 1-6 ikke finder anvendelse ved mikrobetalingsinstrumenter, der anvendes anonymt, eller hvis betalers udbyder på grund af mikrobetalingsinstrumentets karakter ikke er i stand til at bevise, at betalingstransaktionen var autoriseret. Det kan endvidere aftales, at stk. 7 og 8 ikke finder anvendelse på mikrobetalingsinstrumenter, hvis det på grund af betalingsinstrumentets karakter ikke er muligt at spærre for brugen af det.

Stk. 11. Stk. 1-6 finder anvendelse på e-penge, medmindre det ikke er muligt for betalers udbyder af e-penge at spærre betalingskontoen eller betalingsinstrumentet."

Af forarbejderne i lovforslag nr. L 119 af 28. januar 2009 til betalingstjenesteloven fra 2009, fremgår bl.a.

"Almindelige bemærkninger.

1. Indledning

...

Forslaget til lov om betalingstjenester implementerer Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (betalingstjenestedirektivet).

...

Direktivet indeholder også hæftelses- og ansvarsregler, som svarer til de gældende danske hæftelses- og ansvarsregler i lov om visse betalingsmidler. Disse regler foreslås på denne baggrund videreført i forslag til lov om betalingstjenester.

...

2. Lov om visse betalingsmidler

...

Der er i loven bestemmelser om hæftelse, som sikrer, at brugerne ikke lider et urimeligt stort tab, hvis betalingsmidlet for eksempel bliver stjålet og derefter misbrugt. Der er desuden bestemmelser om, hvornår en udsteder af betalingskort er ansvarlig for tab, som brugerne får på grund af fejl i betalingssystemet. Herudover er der regler om tilsyn, idet det skal påses, at sikkerheden i betalingssystemerne er forsvarlig, og at loven i øvrigt overholdes.

...

Det foreslås at videreføre det gældende udgangspunkt i lov om visse betalingsmidler om, at udstederen i forhold til forbrugeren skal bære tabet som følge af misbrug af kortet. Endvidere foreslås den gældende regel videreført, hvorefter en forbruger hæfter med op til 1.200 kr. som følge af andres uberettigede anvendelse af betalingsmidlet, hvis for eksempel pinkoden er anvendt. I helt særlige tilfælde hæfter en forbruger med op til 8.000 kr., når forbrugeren ved, at dennes betalingskort er stjålet, men undlader at spærre kortet.

...

Bemærkninger til lovforslagets enkelte bestemmelser.

...

Til § 57

Det foreslås i § 57, *stk. 1*, at en betalingstransaktion kun er autoriseret, hvis betaleren har meddelt samtykke til at gennemføre betalingstransaktionen. Betaleren kan autorisere en betalingstransaktion før eller, hvis det er aftalt mellem betaleren og dennes udbyder, efter gennemførelsen af betalingstransaktionen. Som eksempler på betalers meddelelse af samtykke kan nævnes, at betaler anvender sin pinkode i en forretning, underskriver en betalingsordre i en filial eller anvender sin kode i en netbank.

Ved »autorisere« forstår godkende. Når lovteksten anvender begrebet autorisere skyldes dette, at begrebet autorisering anvendes i praksis ved gennemførelse af betalingstransaktioner.

Det er en forudsætning for, at en transaktion kan autoriseres efterfølgende, at der forinden er indgået en specifik aftale herom mellem betaler og udbyder. Det beror på en konkret vurdering, hvorvidt der i det enkelte tilfælde er indgået en sådan aftale. Hvis det aftales i rammeaftalen, at betaleren er forpligtet til at autorisere en betalingstransaktion efter, at den er gennemført, vil et sådant vilkår blive anset for at være et urimeligt aftalevilkår. Det kan konkret aftales, at et sådant samtykke kan afgives ved stiltiende accept.

Det er en følge af bestemmelsen, at hvis en betaler ikke har meddelt samtykke til at gennemføre betalingstransaktionen, er betalingstransaktionen uautoriseret, jf. også direktivets art. 54, stk. 2, 2. pkt.

Efter forslaget til *stk. 2* skal et samtykke meddeles i den form og efter den procedure, der er aftalt mellem betaleren og hans udbyder. Bestemmelsen fastsætter derimod ikke krav om, at et samtykke skal meddeles i en bestemt form eller efter en bestemt procedure. Dette spørgsmål er derfor overladt til parternes aftale.

Ifølge forslagets *stk. 3*, kan et samtykke ikke tilbagekaldes efter det tidspunkt, der er følger af forslagets § 73. § 73 fastsætter tidspunktet for, hvornår en betalingstransaktion kan tilbagekaldes. Det betyder for eksempel, at et samtykke til at gennemføre en konto til konto overførsel ikke kan tilbagekaldes efter, at betalingsordren er modtaget af betalers udbyder.

Forslaget til § 57 gennemfører direktivets art. 54.

Til § 61

Det foreslås i § 61, *stk. 1*, at betalers udbyder hæfter i forhold til betaler for tab som følge af uautoriserede betalingstransaktioner, jf. § 57, medmindre andet følger af § 62. Ved en uautoriseret transaktion, skal betalers udbyder straks tilbagebetale betaleren beløbet.

Bestemmelsen finder anvendelse for alle betalingstransaktioner omfattet af lovforslagets bilag 1, og fastslår, at betalers udbyder skal hæfte i forhold til betaler for tab som følge af uautoriserede betalingstransaktioner.

...

...

Til § 62

Med forslaget til § 62 fastlægges den ansvarsfordeling, som skal gælde, hvis et betalingsinstrument bruges af en person, som ikke er berettiget til at bruge det. Bestemmelsen viderefører de hidtil gældende regler i lov om visse betalingsmidler § 11.

...

Det fremgår endvidere af den foreslåede bestemmelse, som er i overensstemmelse med direktivets art. 61, at betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af, at betaler har handlet svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser efter forslaget § 59. Selvom dette ikke fremgår udtrykkeligt af den nuværende § 11 i lov om visse betalingsmidler, må det dog antages, at betaler ud fra almindelige erstatningsretlige regler vil blive pålagt erstatningsansvar, hvis han har handlet svigagtigt overfor sin udbyder. Heller ikke tilføjjelsen om forsætlig overtrædelse af forslaget § 59 forventes at medføre et øget ansvar i forhold til, hvad der følger af den gældende § 11 i lov om visse betalingsmidler.

Selvrisikoreglen på 1.200 kr. i forslaget til *stk. 2* er med en sproglig tilretning identisk med lov om visse betalingsmidler § 11, *stk. 2*. I stedet for den til betalingsmidlet hørende personlige, hemmelige kode er anvendt begrebet den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning. Dette begreb svarer til direktivets »personaliserede sikkerhedsfeatures« og kan for eksempel være en pinkode. Ved at anvende dette begreb i forbindelse med selvrisikoreglen vil denne regel også finde anvendelse, når et betalingsinstrument er anvendt sammen med andre sikkerhedsforanstaltninger, der har samme funktion som en personlig kode. Ved en personlig sikkerhedsforanstaltning forstås en sikkerhedsforanstaltning, der har til formål at sikre en særlig sikker brug af et betalingsinstrument. Det kan være en pinkode, men der er også andre personlige sikkerhedsforanstaltninger som for eksempel fingeraftryk og aflæsning af iris. Der er derimod ikke tale om et til betalingsinstrumentet hørende personlig sikkerhedsforanstaltning, hvis denne foranstaltning er tilgængelig på selve betalingsmidlet.

En underskrift betragtes heller ikke som en personlig sikkerhedsforanstaltning.

Det forudsættes som hidtil, at selvriskoen ikke vil blive gjort gældende af en udbyder over for en betaler i situationer, hvor det vil være klart stødende at lade betaleren hæfte, for eksempel når betalingsmidlet og koden er fratrundet betaleren ved anvendelse af vold eller trussel om vold.

...

De tilfælde efter *stk. 3, nr. 1-3*, hvor brugeren hæfter, omhandler alene brugerens manglende påpasselighed ved omgangen med den personlige sikkerhedsforanstaltning. Bestemmelsen understøtter herved, at der er tale om en personlig sikkerhedsforanstaltning, som ikke må overdrages til eller bruges af andre.

...

Betaleren hæfter uden beløbsbegrænsning for tab, når den, der uberettiget har anvendt betalingsinstrumentet, har brugt den til betalingsinstrumentet hørende personlige sikkerhedsforanstaltning og betalers udbyder kan godtgøre, at betaleren har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget misbruget. Det skal samtidig være sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug."

Betalingstjenestedirektiverne

I Europa-Parlamentets og Rådets i dag ophævede direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (første betalingstjenestedirektiv) står der bl.a.:

"(32) For at opmuntre brugeren af betalingstjenester til snarest muligt at underrette udbyderen om et eventuelt tyveri eller tab af et betalingsinstrument og således mindske risikoen for uautoriserede betalingstransaktioner, bør brugeren kun holdes ansvarlig for et begrænset beløb, medmindre brugeren af betalingstjenester har handlet svigagtigt eller groft forsømmeligt. Når brugeren har meddelt udbyderen af betalingstjenester, at hans betalingsinstrument kan være misbrugt, bør brugeren ikke længere skulle dække tab som følge af uautoriseret brug af instrumentet. Dette direktiv bør ikke berøre udbyderen af betalingstjenesters ansvar for den tekniske sikkerhed vedrørende egne produkter.

(33) For at vurdere eventuel forsømmelse fra brugeren af betalingstjenester bør der tages hensyn til alle omstændigheder. Beviset for og graden af den påståede forsømmelse bør vurderes i henhold til national ret. Aftalevilkår og betingelser vedrørende levering og brug af et betalingsinstrument, som pålægger forbrugeren en større bevisbyrde, eller som reducerer udstederens bevisbyrde, bør betragtes som ugyldige.

(34) Medlemsstaterne bør dog kunne fastsætte mindre strenge bestemmelser end de ovenfor omhandlede for at bevare det nuværende niveau af forbrugerbeskyttelse og fremme tilliden til, at det er sikkert at bruge elektroniske betalingsinstrumenter. Der bør tages passende hensyn til det forhold, at forskellige betalingsinstrumenter indebærer forskellige risici, hvilket fremmer udstedelsen af sikrere instrumenter.

Medlemsstaterne bør kunne begrænse eller helt ophæve betalerens ansvar, medmindre denne har optrådt svigagtigt.

(35) Der bør indføres bestemmelser om fordeling af tab i tilfælde af uautoriserede betalingstransaktioner. Der kan gælde andre bestemmelser for brugere af betalingstjenester, der ikke er forbrugere, idet sådanne brugere normalt har større mulighed for at vurdere risikoen for svig og træffe modforanstaltninger.

(36) Dette direktiv bør fastsætte regler om tilbagebetaling, der beskytter forbrugeren, når den gennemførte betalingstransaktion overstiger det beløb, der med rimelighed kunne forventes. Udbydere af betalingstjenester bør kunne tilbyde deres kunder endnu gunstigere vilkår og f.eks. tilbagebetale enhver betalingstransaktion, der omtvistet. Hvis brugeren kræver tilbagebetaling af en betalingstransaktion, bør retten til tilbagebetaling hverken påvirke betalerens ansvar over for betalingsmodtageren fra det underliggende forhold, f.eks. hvad angår varer og tjenester, som er bestilt, forbrugt eller retmæssigt faktureret, eller brugerens retigheder hvad angår tilbagekaldelse af en betalingsordre.

...

KAPITEL 2

Autorisation af betalingstransaktioner

Artikel 54

Samtykke og tilbagekaldelse af samtykke

1. Medlemsstaterne sikrer, at en betalingstransaktion kun anses for at være autoriseret, hvis betaleren har meddelt sit samtykke til at gennemføre betalingstransaktionen. Betaleren kan autorisere en betalingstransaktion før eller, hvis det er aftalt mellem betaleren og hans udbyder af betalingstjenester, efter gennemførelsen af betalingstransaktionen.

2. Samtykke til at gennemføre en betalingstransaktion eller en række betalingstransaktioner meddeles i den form, der er aftalt mellem betaleren og hans udbyder af betalingstjenester.

Hvis dette samtykke mangler, anses betalingstransaktionen for uautoriseret.

3. Betaleren kan til enhver tid tilbagekalde et samtykke, men ikke senere end det tidspunkt for uigenkaldelighed, der er omhandlet i artikel 66. Et samtykke til at gennemføre en række betalingstransaktioner, kan også tilbagekaldes, med den virkning, at eventuelle fremtidige betalingstransaktioner skal anses for uautoriserede.

4. Betaleren og udbyderen af betalingstjenester træffer aftale om proceduren for meddelelse af samtykke.

...

Artikel 60

Udbyderens ansvar for uautoriserede betalingstransaktioner

1. Medlemsstaterne sikrer, at betalerens udbyder af betalingstjenester med forbehold af artikel 58 i tilfælde af en uautoriseret betalingstransaktion straks tilbagebetaler betaleren beløbet for den uautoriserede betalingstransaktion og, hvor det er relevant, fører den debiterede betalingskonto tilbage til den situation, der ville have været gældende, hvis den uautoriserede betalingstransaktion ikke var blevet gennemført.

2. Yderligere økonomisk godtgørelse kan fastsættes i overensstemmelse med den lovgivning, der finder anvendelse på aftalen mellem betaleren og dennes udbyder af betalingstjenester.

Artikel 61

Betalerens ansvar for uautoriserede betalingstransaktioner

1. Uanset artikel 60 skal betaleren dække tab i forbindelse med enhver uautoriseret betalingstransaktion på højst 150 EUR, der skyldes brug af et tabt eller stjålet betalingsinstrument eller, hvis betaleren har undladt at beskytte de personaliserede sikkerhedsfeatures, uberettiget tilegnelse af et betalingsinstrument.
2. Betaleren skal dække alle tab som følge af uautoriserede betalingsstransaktioner, hvis de skyldes en svigagtig handling eller manglende opfyldelse af en eller flere af hans forpligtelser i henhold til artikel 56 ved forsæt eller grov forsømmelse. I sådanne tilfælde finder maksimumbeløbet i stk. 1 i nærværende artikel ikke anvendelse.
3. I de tilfælde, hvor betaleren ikke har optrådt svigagtigt eller med forsæt har undladt at opfylde sine forpligtelser i henhold til artikel 56, kan medlemsstaterne begrænse det i stk. 1 og 2 i nærværende artikel omhandlede ansvar under hensyntagen til navnlig arten af betalingsinstrumentets personaliserede sikkerhedsfeatures og de omstændigheder, under hvilke det blev tabt, stjålet eller uberettiget tilegnet.
4. Betaleren skal ikke dække økonomiske følger af brug af et tabt, stjålet eller uberettiget tilegnet betalingsinstrument, efter at der er sket underretning i overensstemmelse med artikel 56, stk. 1, litra b), undtagen hvis betaleren har optrådt svigagtigt.
5. Hvis udbyderen af betalingstjenester ikke træffer egnede foranstaltninger til på alle tidspunkter at kunne modtage underretning om tabte, stjålne eller uberettiget tilegnede betalingsinstrumenter som anført i artikel 57, stk. 1, litra c), hæfter betaleren ikke for de økonomiske følger af brug af betalingsinstrumentet, undtagen hvis han har handlet svigagtigt."

Af Europa-Parlamentets og Rådets Direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (andet betalingstjenestedirektiv) fremgår bl.a.:

"(7) I de senere år er de sikkerhedsrisici, der er forbundet med elektroniske betalinger, blevet større. Dette skyldes deres voksende tekniske kompleksitet, de stadigt stigende mængder af elektroniske betalinger i verden og nye typer betalingstjenester. Sikre betalingstjenester er en forudsætning for et velfungerende betalingstjenestemarked. Betalingstjenestebrugere bør derfor være tilstrækkeligt beskyttede mod sådanne risici. Betalingstjenester er nødvendige for funktionaliteten af centrale økonomiske og sociale aktiviteter.

...

(69) Forpligtelsen til at beskytte personaliserede sikkerhedsoplysninger er af afgørende betydning for at beskytte betalingstjenestebrugers midler og for at begrænse risici vedrørende svig og uautoriseret adgang

til betalingskonti. Imidlertid bør vilkår og betingelser eller andre forpligtelser, som betalingstjenesteudbydere pålægger betalingstjenestebrugere med henblik på at beskytte personaliserede sikkerhedsoplysninger, ikke udformes på en sådan måde, at betalingstjenestebrugere forhindres i at drage fordel af tjenesteydelser, som tilbydes af andre betalingstjenesteudbydere, herunder betalingsinitieringstjenester og kontooplysningstjenester. Endvidere bør sådanne vilkår og betingelser ikke indeholde bestemmelser, der på nogen måde vil gøre det vanskeligere at anvende betalingstjenester hos andre betalingstjenesteudbydere, der er meddelt tilladelse eller registreret i henhold til dette direktiv.

(70) Med henblik på at begrænse risiciene for og konsekvenserne af uautoriserede eller fejlbehæftede betalingstransaktioner bør betalingstjenestebrugeren så hurtigt som muligt orientere betalingstjenesteudbyderen om eventuelle indsigelser, der gøres mod betalingstransaktioner, som angiveligt er uautoriserede eller fejlbehæftede, forudsat at betalingstjenesteudbyderen har opfyldt sine oplysningsforpligtelser efter dette direktiv. Hvis betalingstjenestebrugeren overholder underretningsfristen, bør betalingstjenestebrugeren kunne påberåbe sig de pågældende krav med forbehold af nationale forældelsesfrister. Dette direktiv bør ikke berøre andre krav mellem betalingstjenestebrugere og betalingstjenesteudbydere.

(71) I tilfælde af en uautoriseret betalingstransaktion bør betalingstjenesteudbyderen straks tilbagebetale transaktionsbeløbet til betaleren. Hvis der er stor mistanke om en uautoriseret transaktion som følge af svigagtig adfærd fra betalingstjenestebrugers side, og mistanken er baseret på objektive grunde, som er meddelt den relevante nationale myndighed, bør betalingstjenesteudbyderen have mulighed for inden for en rimelig frist at foretage en undersøgelse før tilbagebetaling til betaleren. For at forhindre, at betaleren stilles ugunstigt, bør valørdatoen for kreditering ikke være senere end den dato, hvor beløbet blev debiteret. For at tilskynde betalingstjenestebrugeren til snarest muligt at underrette betalingstjenesteudbyderen om et eventuelt tyveri eller tab af et betalingsinstrument og således mindske risikoen for uautoriserede betalingstransaktioner bør brugeren kun hæfte for et begrænset beløb, medmindre betalingstjenestebrugeren har handlet svigagtigt eller groft forsømmeligt. I denne sammenhæng synes et beløb på 50 EUR at være tilstrækkeligt for at sikre en harmoniseret og omfattende brugerbeskyttelse i Unionen.

Der bør ikke pålægges ansvar, hvis betaleren ikke er i stand til at opdage tabet, tyveriet eller den uberettigede tilegnelse af betalingsinstrumentet. Når brugeren har meddelt betalingstjenesteudbyderen, at vedkommendes betalingsinstrument kan være misbrugt, bør betalingstjenestebrugeren desuden ikke skulle dække yderligere tab som følge af uautoriseret brug af instrumentet. Dette direktiv bør ikke berøre betalingstjenesteudbyderes ansvar for den tekniske sikkerhed af deres egne produkter.

(72) For at vurdere eventuel forsømmelse eller grov forsømmelse fra betalingstjenestebrugers side bør der tages hensyn til alle omstændigheder. Beviset for og graden af den påståede forsømmelse bør generelt

vurderes i henhold til national ret. Selv om begrebet forsømmelse indebærer tilsidesættelse af diligenspligten, bør grov forsømmelse imidlertid indebære mere end blot forsømmelse og vedrøre adfærd, der involverer en betydelig grad af skødesløshed, f.eks. opbevaring af de sikkerhedsoplysninger, der anvendes til at give tilladelse til en betalingstransaktion, ved siden af betalingsinstrumentet i et format, der på en åben og let måde kan opdages af tredjeparter. Aftalevilkår og betingelser vedrørende levering og brug af et betalingsinstrument, som pålægger forbrugeren en større bevisbyrde, eller som reducerer udstederens bevisbyrde, bør betragtes som ugyldige. Ydermere er det i specifikke situationer, navnlig hvis betalingsinstrumentet ikke er til stede ved salgsstedet, som ved onlinebetalinger, hensigtsmæssigt, at betalingstjenesteudbyderen er forpligtet til at forelægge beviser for angivelig forsømmelighed, da betalerens mulighed for at gøre dette er meget begrænset i sådanne tilfælde.

(73) Der bør indføres bestemmelser om fordeling af tab i tilfælde af uautoriserede betalingstransaktioner. Der kan gælde andre bestemmelser for betalingstjenestebrugere, der ikke er forbrugere, idet sådanne brugere normalt har større mulighed for at vurdere risikoen for svig og træffe modforanstaltninger. For at sikre en høj grad af forbrugerbeskyttelse bør betalere altid være berettiget til at rette deres krav om tilbagebetaling til deres kontoførende betalingstjenesteudbyder, også selv om en betalingsinitieringstjenesteudbyder er involveret i betalingstransaktionen. Dette berører ikke fordelingen af ansvar mellem betalingstjenesteudbyderne.

...

KAPITEL 2

Autorisation af betalingstransaktioner

Artikel 64

Samtykke og tilbagekaldelse af samtykke

1. Medlemsstaterne sikrer, at en betalingstransaktion kun anses for at være autoriseret, hvis betaleren har meddelt sit samtykke til at gennemføre betalingstransaktionen. Betaleren kan autorisere en betalingstransaktion før eller, hvis det er aftalt mellem betaleren og dennes betalingstjenesteudbyder, efter gennemførelsen af betalingstransaktionen.
2. Samtykke til at gennemføre en betalingstransaktion eller en række betalingstransaktioner meddeles i den form, der er aftalt mellem betaleren og dennes betalingstjenesteudbyder. Samtykke til at gennemføre en betalingstransaktion kan også gives via betalingsmodtageren eller betalingsinitieringstjenesteudbyderen. Hvis der ikke er meddelt samtykke, anses betalingstransaktionen for uautoriseret.
3. Betaleren kan til enhver tid tilbagekalde et samtykke, men ikke senere end på tidspunktet for uigenkaldelighed, jf. artikel 80. Et samtykke til at gennemføre en række betalingstransaktioner kan også tilbagekaldes, hvorefter eventuelle fremtidige betalingstransaktioner skal anses for at være uautoriserede.
4. Betaleren og betalingstjenesteudbyderne træffer aftale om proceduren for meddelelse af samtykke.

...

*Artikel 73***Betalingstjenesteudbyderes ansvar for uautoriserede betalingstransaktioner**

1. Medlemsstaterne sikrer med forbehold af artikel 71, at en betalers betalingstjenesteudbyder i tilfælde af en uautoriseret betalingstransaktion tilbagebetaler betaleren beløbet for den uautoriserede betalingstransaktion straks og under alle omstændigheder inden afslutningen af den følgende arbejdsdag efter at have konstateret eller være blevet underrettet om transaktionen, medmindre betalerens betalingstjenesteudbyder har rimelige grunde til at have mistanke om svig og skriftligt underretter den relevante nationale myndighed om disse grunde. Betalerens betalingstjenesteudbyder skal i givet fald føre den debiterede betalingskonto tilbage til den situation, der ville have været gældende, hvis den uautoriserede betalingstransaktion ikke var blevet gennemført. Herved skal det også sikres, at valørdatoen for kreditering af betalerens betalingskonto ikke ligger senere end den dato, hvor beløbet blev debiteret.
2. Hvis betalingstransaktionen initieres via en betalingsinitieringstjenesteudbyder, skal den kontoførende betalingstjenesteudbyder straks og under alle omstændigheder inden afslutningen af den følgende arbejdsdag tilbagebetale beløbet for den uautoriserede betalingstransaktion og, hvor det er relevant, føre den debiterede betalingskonto tilbage til den situation, der ville have været gældende, hvis den uautoriserede betalingstransaktion ikke var blevet gennemført.
Hvis betalingsinitieringstjenesteudbyderen er ansvarlig for den uautoriserede betalingstransaktion, skal denne efter den kontoførende betalingstjenesteudbyders anmodning herom straks holde denne skadesløs for tab eller betalte beløb som følge af tilbagebetalingen til betaleren, herunder beløbet for den uautoriserede betalingstransaktion. I overensstemmelse med artikel 72, stk. 1, er det betalingsinitieringstjenesteudbyderen, der inden for sit kompetenceområde bærer bevisbyrden for, at betalingstransaktionen var autentificeret, korrekt registreret og ikke ramt af tekniske svigt eller andre fejl i tilknytning til den betalingstjeneste, som betalingsinitieringstjenesteudbyderen har ansvaret for.
3. Yderligere finansiell kompensation kan fastsættes i overensstemmelse med den lovgivning, der finder anvendelse på den aftale, der er indgået mellem betaleren og betalingstjenesteudbyderen, eller den aftale, der er indgået mellem betaleren og betalingsinitieringstjenesteudbyderen, hvor det er relevant.

*Artikel 74***Betalers ansvar for uautoriserede betalingstransaktioner**

1. Uanset artikel 73 kan en betaler forpligtes til at dække tab i forbindelse med enhver uautoriseret betalingstransaktion på op til 50 EUR, der skyldes brug af et tabt eller stjålet betalingsinstrument eller uberettiget tilegnelse af et betalingsinstrument.
Første afsnit finder ikke anvendelse, hvis:
 - a) tabet, tyveriet eller den uberettigede tilegnelse af betalingsinstrumentet ikke kunne opdages af betaleren forud for betalingen, medmindre betaleren selv har handlet svigagtigt, eller

b) tabet er forårsaget af handlinger, der er foretaget af en betalingstjenesteudbyders ansat, agent eller filial eller en enhed, hvortil dens aktiviteter er outsourcet, eller disses passivitet.

Betaleren skal dække alle tab som følge af uautoriserede betalingstransaktioner, hvis de skyldes betalerens svigagtige handling eller manglende opfyldelse af en eller flere af de forpligtelser, der er fastsat i artikel 69, begået med forsæt eller ved grov forsømmelse. I sådanne tilfælde finder maksimumsbeløbet i første afsnit ikke anvendelse.

...

KAPITEL 5

Drifts- og sikkerhedsrisici og autentifikation

Artikel 95

Styring af drifts- og sikkerhedsrisici

1. Medlemsstaterne sikrer, at betalingstjenesteudbydere fastlægger en ramme med passende begrænsende foranstaltninger og kontrolmekanismer til styring af drifts- og sikkerhedsrisici, der er forbundet med de betalingstjenester, som de udbyder. Som en del af denne ramme fastlægger og opretholder betalingstjenesteudbydere effektive procedurer for håndtering af hændelser, herunder for opdagelse og klassificering af større drifts- og sikkerhedshændelser.

2. Medlemsstaterne sikrer, at betalingstjenesteudbydere årligt eller oftere som fastsat af den kompetente myndighed giver den kompetente myndighed en ajourført samlet vurdering af de drifts- og sikkerhedsrisici, der er forbundet med de betalingstjenester, som de udbyder, og om, hvorvidt de iværksatte begrænsende foranstaltninger og kontrolmekanismer som følge af disse risici er tilstrækkelige.

3. Senest den 13. juli 2017 udarbejder EBA i tæt samarbejde med ECB efter høring af alle relevante interessenter, herunder interessenter på betalingstjenestemarkedet, og under hensyntagen til alle involverede interesser retningslinjer i overensstemmelse med artikel 16 i forordning (EU) nr. 1093/2010 for fastlæggelse, iværksættelse og overvågning af sikkerhedsforanstaltninger, herunder certificeringsprocesser, hvor det er relevant.

EBA gennemgår i tæt samarbejde med ECB de i første afsnit omhandlede retningslinjer regelmæssigt og under alle omstændigheder mindst hvert andet år.

4. Under hensyntagen til den indhøstede erfaring fra anvendelsen af de i stk. 3 omhandlede retningslinjer udarbejder EBA på Kommissionens foranledning, hvis det er relevant, udkast til reguleringsmæssige tekniske standarder om kriterier og betingelser for fastlæggelse og overvågning af sikkerhedsforanstaltninger.

Kommissionen tillægges beføjelse til at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010.

5. EBA fremmer samarbejde, herunder udveksling af oplysninger, inden for drifts- og sikkerhedsrisici i forbindelse med betalingstjenester mellem de kompetente myndigheder samt mellem de kompetente

myndigheder og ECB og, hvor det er relevant, Den Europæiske Unions Agentur for Net- og Informationssikkerhed.

Artikel 96

Indberetning af hændelser

1. I tilfælde af en større drifts- eller sikkerhedshændelse underretter betalingstjenesteudbydere uden unødigt forsinkelse den kompetente myndighed i betalingstjenesteudbyderens hjemland.

Hvis hændelsen har eller kan have indvirkning på betalingstjenesteudbyderens betalingstjenestebrugeres økonomiske interesser, orienterer betalingstjenesteudbyderen uden unødigt forsinkelse sine betalingstjenestebrugere om hændelsen og om alle tilgængelige foranstaltninger, som de kan træffe for at begrænse hændelsens negative følger.

2. Ved modtagelsen af underretningen omhandlet i stk. 1 fremsender den kompetente myndighed i hjemlandet uden unødigt forsinkelse relevante oplysninger om hændelsen til EBA og ECB. Denne kompetente myndighed underretter, efter at have vurderet hændelsens relevans for de relevante myndigheder i den på gældende medlemsstat, disse herom.

EBA og ECB vurderer i samarbejde med den kompetente myndighed i hjemlandet hændelsens relevans for andre relevante EU-myndigheder og nationale myndigheder og underretter dem i overensstemmelse hermed. ECB underretter medlemmerne af Det Europæiske System af Centralbanker om spørgsmål, der er relevante for betalingssystemet.

De kompetente myndigheder træffer på grundlag af underretningen, hvis det er hensigtsmæssigt, alle nødvendige foranstaltninger for at beskytte det finansielle systems umiddelbare sikkerhed.

3. Senest den 13. januar 2018 udsteder EBA i tæt samarbejde med ECB efter høring af alle relevante interessenter, herunder interessenter på betalingstjenestemarkedet, og under hensyntagen til alle involverede interesser retningslinjer i overensstemmelse med artikel 16 i forordning (EU) nr. 1093/2010 adresseret til hver af følgende:

- a) til betalingstjenesteudbydere om klassificering af større hændelser som omhandlet i stk. 1 og om indholdet og formatet af, herunder standardunderretningsmodeller, og procedurerne for underretning om sådanne hændelser
- b) til de kompetente myndigheder om kriterierne for, hvordan det skal vurderes, hvor relevant en hændelse er, og hvilke elementer i hændelsesindberetningerne der skal deles med andre nationale myndigheder.

4. EBA gennemgår i tæt samarbejde med ECB de i stk. 3 omhandlede retningslinjer regelmæssigt og under alle omstændigheder mindst hvert andet år.

5. EBA tager i forbindelse med udstedelsen og gennemgangen af de i stk. 3 omhandlede retningslinjer hensyn til standarder og/eller specifikationer, som er udarbejdet og offentliggjort af Den Europæiske Unions Agentur for Net- og Informationssikkerhed for de sektorer, der udøver andre aktiviteter end udbud af betalingstjenester.

6. Medlemsstaterne sikrer, at betalingstjenesteudbydere mindst en gang om året stiller statistiske data om svig i tilknytning til forskellige betalingsmidler til rådighed for deres kompetente myndigheder. Disse

kompetente myndigheder stiller sådanne data til rådighed for EBA og ECB i sammenfattet form.

Artikel 97

Autentifikation

1. Medlemsstaterne sikrer, at en betalingstjenesteudbyder anvender stærk kundeautentifikation, når betaleren:
 - a) tilgår sin betalingskonto online
 - b) initierer en elektronisk betalingstransaktion
 - c) udfører handlinger gennem en fjernkanal, der kan indebære en risiko for betalingssvig eller andre former for misbrug.
2. Men henblik på initiering af elektroniske betalingstransaktioner, jf. stk. 1, litra b), sikrer medlemsstaterne, at betalingstjenesteudbydere, for så vidt angår elektroniske fjernbetalingstransaktioner, anvender stærk kundeautentifikation, som omfatter elementer, der dynamisk knytter transaktionen til et specifikt beløb og en specifik betalingsmodtager.
3. Med henblik på stk. 1 sikrer medlemsstaterne, at betalingstjenesteudbydere har iværksat passende sikkerhedsforanstaltninger for at beskytte fortroligheden og integriteten af betalingstjenestebrugeres personaliserede sikkerhedsoplysninger.
4. Stk. 2 og 3 finder også anvendelse, når betalinger initieres via en betalingsinitieringstjenesteudbyder. Stk. 1 og 3 finder også anvendelse, når der anmodes om oplysningerne via en kontooplysningstjenesteudbyder.
5. Medlemsstaterne sikrer, at den kontoførende betalingstjenesteudbyder giver betalingsinitieringstjenesteudbyderen og kontooplysningstjenesteudbyderen tilladelse til at anvende de autentifikationsprocedurer, som den kontoførende betalingstjenesteudbyder stiller til rådighed for betalingstjenestebrugeren i overensstemmelse med stk. 1 og 3, og, såfremt betalingsinitieringstjenesteudbyderen er involveret, i overensstemmelse med stk. 1, 2 og 3.

Artikel 98

Reguleringsmæssige tekniske standarder for autentifikation og kommunikation

1. EBA udarbejder i tæt samarbejde med ECB efter høring af alle relevante interessenter, herunder interessenter på betalingstjenestemarkedet, og under hensyntagen til alle involverede interesser udkast til reguleringsmæssige tekniske standarder til betalingstjenesteudbydere som fastsat i dette direktivs artikel 1, stk. 1, i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 vedrørende:
 - a) krav til stærk kundeautentifikation, jf. artikel 97, stk. 1 og 2
 - b) undtagelser fra anvendelsen af artikel 97, stk. 1, 2 og 3, på grundlag af de i nærværende artikels stk. 3 fastsatte kriterier
 - c) krav, som sikkerhedsforanstaltninger skal opfylde, i overensstemmelse med artikel 97, stk. 3, for at beskytte fortroligheden og integriteten af betalingstjenestebrugeres personaliserede sikkerhedsoplysninger, og
 - d) krav til fælles og sikre åbne standarder for kommunikation mellem kontoførende betalingstjenesteudbydere, betalingsinitieringstjenesteudbydere, kontooplysningstjenesteudbydere, betalere,

betalingsmodtagere og andre betalingstjenesteudbydere med henblik på identifikation, autentifikation, underretning og udveksling af oplysninger samt iværksættelse af sikkerhedsforanstaltninger.

2. De i stk. 1 omhandlede udkast til reguleringsmæssige tekniske standarder udarbejdes af EBA med henblik på at:
 - a) sikre en passende grad af sikkerhed for betalingstjenestebrugere og betalingstjenesteudbydere ved at indføre effektive og risikobaserede krav
 - b) sikre betalingstjenestebrugeres midler og personoplysninger
 - c) sikre og opretholde fair konkurrence mellem alle betalingstjenesteudbydere
 - d) sikre teknologi- og forretningsmodelneutralitet
 - e) gøre det muligt at udvikle brugervenlige, tilgængelige og innovative betalingsmidler.
3. De i stk. 1, litra b), omhandlede undtagelser skal bygge på følgende kriterier:
 - a) risikoniveauet for den tjeneste, der udbydes
 - b) transaktionens beløb, tilbagevendende karakter eller begge dele
 - c) den betalingskanal, der anvendes til at gennemføre transaktionen.
4. EBA forelægger de i stk. 1 omhandlede udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 13. januar 2017. Kommissionen tillægges beføjelse til at vedtage de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i forordning (EU) nr. 1093/2010.
5. EBA gennemgår og ajourfører om nødvendigt regelmæssigt de reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010 for bl.a. at tage højde for innovation og den teknologiske udvikling."

Der er i medfør af artikel 98 udstedt Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation. De heri indeholdte regler angår ikke og stiller ikke krav om, at betalingstjenesteudbydere skal indrette deres systemer på en sådan måde, at der advares om usædvanlige overførsler fra betalere og/eller at sådanne overførsler automatisk stoppes.

I det endnu ikke gennemførte forslag til Europa-Parlamentets og Rådets forordning om betalingstjenester i det indre marked og om ændring af forordning (EU) nr. 1093/2010, COM(2023) 366, er det indledningsvis anført bl.a. (fodnoter udeladt):

"1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Det andet betalingstjenestedirektiv (PSD2)¹ udgør en retlig ramme for alle detailbetalinger i EU, både i euro og andre valutaer, både indenlandske og grænseoverskridende. Det første betalingstjenestedirektiv, der blev vedtaget i 2007, fastlagde en harmoniseret retlig ramme for oprettelsen af et integreret EU-betalingsmarked.

...

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEENTER OG KONSEKVENSANALYSER

• Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning

Der blev foretaget en evaluering af det andet betalingstjenestedirektiv i 2022. Input til evalueringen omfattede en rapport fra en uafhængig kontrahent og interessenterne synspunkter i forskellige offentlige høringer. Evalueringsrapporten offentliggøres som bilag til den konsekvensanalyse, der ledsager dette forslag.

I evalueringsrapporten konkluderes det, at det andet betalingstjenestedirektiv har haft forskellige grader af succes med hensyn til at opfylde målene. Et område med positive virkninger har været forebyggelse af svig via indførelsen af stærk kundeautentifikation."

I den foreslåede forordning er det anført:

" ...

(1) Siden vedtagelsen af Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 har detailmarkedet for betalingstjenester undergået betydelige ændringer, hovedsagelig i forbindelse med den stigende brug af kort og andre digitale betalingsmidler, den faldende brug af kontanter og den stigende tilstedeværelse af nye aktører og tjenester, herunder digitale tegnebøger og kontaktløse betalinger. Covid-19-pandemien og de forandringer, den har medført for forbrugs- og betalingspraksis, har øget betydningen af at have sikre og effektive betalinger.

(2) I Kommissionens meddelelse om en detailbetalingsstrategi for EU³⁴ bebudes det, at der vil blive iværksat en omfattende gennemgang af anvendelsen og virkningen af direktiv (EU) 2015/2366, "*som bør omfatte en samlet vurdering af, om det stadig er egnet til formålet, under hensyntagen til markedsudviklingen*".

(3) Direktiv (EU) 2015/2366 havde til formål at fjerne hindringer for nye typer betalingstjenester og forbedre forbrugerbeskyttelsen og -sikkerheden. Kommissionens evaluering af virkningen og anvendelsen af direktiv (EU) 2015/2366 viste, at direktiv (EU) 2015/2366 i vid udstrækning har været vellykket med hensyn til mange af dets mål, men identificerede også visse områder, hvor direktivets mål ikke er nået fuldt ud. F.eks. pegede evalueringen på stigningen i nye former for svig som et problem, der giver anledning til bekymring med hensyn til forbrugerbeskyttelsesmål. Der er også konstateret mangler med hensyn til målet om at forbedre konkurrencen på markedet takket være de såkaldte "open banking-tjenester" (kontooplysningstjenester og betalingsinitieringstjenester) ved at mindske de markedshindringer, som tredjepartsudbydere står over for. Fremskridtene hen imod målet om at forbedre udbuddet af grænseoverskridende betalingstjenester har også været begrænsede, hovedsagelig på grund af uoverensstemmelser i tilsynspraksis og håndhævelse i hele Unionen. Evalueringen identificerede også

faktorer, der hæmmer fremskridtene med hensyn til målet om at skabe lige vilkår for alle udbydere af betalingstjenester.

(4) Evalueringen afdækkede også problemer med forskellig gennemførelse og håndhævelse af direktiv (EU) 2015/2366, som direkte påvirker konkurrencen mellem betalingstjenesteudbydere ved at skabe forskellige lovgivningsmæssige betingelser i de forskellige medlemsstater og tilskynde til regelarbitrage.

...

(75) Der bør fastsættes bestemmelser om fordeling af tab i tilfælde af uautoriserede betalingstransaktioner eller specifikke autoriserede kreditoverførsler. Der kan gælde andre bestemmelser for brugere af betalingstjenester, der ikke er forbrugere, idet sådanne brugere normalt har større mulighed for at vurdere risikoen for svig og træffe modforanstaltninger. For at sikre en høj grad af forbrugerbeskyttelse bør betalere altid være berettiget til at rette deres krav om tilbagebetaling til deres kontoførende betalingstjenesteudbyder, også selv om en betalingsinitieringstjenesteudbyder er involveret i betalingstransaktionen. Dette bør ikke berøre fordelingen af ansvar mellem betalingstjenesteudbyderne.

...

(79) Forbrugerne bør beskyttes tilstrækkeligt i forbindelse med visse svigagtige betalingstransaktioner, som de har givet tilladelse til uden at vide, at disse transaktioner var svigagtige. Antallet af "social engineering"-sager, hvor forbrugere vildledes til at godkende en betalingstransaktion til en svindler, er steget markant i de senere år. "Spoofing"-tilfælde, hvor svindlere foregiver at være ansatte hos en kundes betalingstjenesteudbyder og misbruger betalingstjenesteudbyderens navn, postadresse eller telefonnummer til at vinde kundernes tillid og få dem til at udføre visse handlinger, bliver desværre mere udbredt i Unionen. Disse nye former for "spoofing"-svig udviser forskellen i direktiv (EU) 2015/2366 mellem autoriserede og uautoriserede transaktioner. De midler, hvormed samtykket kan antages at være givet, bliver også mere komplekse at identificere, da svindlere kan tage kontrol over hele samtykke- og autentifikationsprocessen, herunder den stærke kundeautentifikation. Der bør tages behørigt hensyn til de betingelser, hvorunder kunden godkendte en transaktion ved at give sin tilladelse hertil, herunder af domstolene, for at kvalificere en transaktion som autoriseret eller uautoriseret. En transaktion kan ganske vist være blevet godkendt under omstændigheder, hvor en sådan tilladelse blev givet på manipulerede præmisser, der påvirkede godkendelsens integritet. Det er derfor ikke længere muligt, som det var tilfældet i direktiv (EU) 2015/2366, at begrænse tilbagebetalinger til uautoriserede transaktioner. Det ville imidlertid være uforholdsmæssigt og økonomisk meget dyrt for betalingstjenesteudbyderne at åbne enhver svigagtig transaktion, hvad enten de er autoriserede eller uautoriserede, for en systematisk ret til tilbagebetaling. Det kan også medføre moralsk risiko og mindske kundens årvågenhed.

(80) Betalingstjenesteudbydere kan også betragtes som ofre for "spoofing"-sager, da deres oplysninger blev misbrugt. Betalingstjenesteudbydere har imidlertid flere midler end forbrugerne til at sætte en stopper

for disse tilfælde af svig gennem passende forebyggelse og solide tekniske sikkerhedsforanstaltninger, der er udviklet i samarbejde med udbydere af elektroniske kommunikationstjenester såsom mobilnetoperatører, internetplatforme osv. Tilfælde af svindel i form af at udgive sig for at være en bankmedarbejder påvirker bankens gode omdømme, banksektoren som helhed og kan forårsage betydelige økonomiske skader for EU's forbrugere, hvilket påvirker deres tillid til elektroniske betalinger og til banksystemet. En forbruger i god tro, som har været offer for en sådan "spoofing"-svindel, hvor svindlere udgiver sig for at være ansatte hos en kundes betalingstjenesteudbyder og misbruger betalingstjenesteudbyderens navn, postadresse eller telefonnummer, bør derfor have ret til at få refunderet det fulde beløb for den svigagtige betalingstransaktion fra betalingstjenesteudbyderen, medmindre betaleren har handlet svigagtigt eller med "grov uagtsomhed". Så snart forbrugeren bliver opmærksom på, at vedkommende har været offer for denne form for "spoofing"-svindel, bør forbrugeren uden unødigt forsinkelse anmelde hændelsen til politiet, helst via onlineklageprocedurer, hvis sådanne stilles til rådighed af politiet, og til sin betalingstjenesteudbyder og fremlægge al nødvendig dokumentation. Der bør ikke ydes refusion, hvis disse proceduremæssige betingelser ikke er opfyldt.

...

(82) For at vurdere eventuel forsømmelse eller grov forsømmelse fra betalingstjenestebrugerens side bør der tages hensyn til alle omstændigheder. Beviset for og graden af den påståede forsømmelse bør generelt vurderes i henhold til national ret. Selv om begrebet uagtsomhed indebærer en tilsidesættelse af omsorgspligten, bør der ved "grov uagtsomhed" forstås mere end blot uagtsomhed, der involverer adfærd, der udviser en betydelig grad af skødesløshed, for eksempel opbevaring af de legitimationsoplysninger, der bruges til at godkende en betalingstransaktion, ved siden af betalingsinstrumentet i et format, der er åbent og let at opdage for tredjeparter. Det faktum, at en forbruger allerede har modtaget en tilbagebetaling fra en betalingstjenesteudbyder efter at være blevet offer for svig ved at nogen har udgivet sig for at være bankansat, og indgiver endnu et tilbagebetalingskrav til den samme betalingstjenesteudbyder efter igen at være blevet offer for den samme type svig, kan betragtes som "grov uagtsomhed", da det kan indikere en høj grad af uforsigtighed fra brugeren, som burde have været mere opmærksom efter allerede at have været offer for den samme svigagtige fremgangsmåde.

...

(100) Svindlere går ofte efter de mest sårbare personer i vores samfund. Rettidig afsløring af svigagtige betalingstransaktioner er afgørende, og overvågning af transaktioner spiller en vigtig rolle i forbindelse med denne afsløring. Det er derfor hensigtsmæssigt at kræve, at betalingstjenesteudbydere har indført mekanismer til overvågning af transaktioner, der afspejler disse mekanismers afgørende bidrag til forebyggelse af svig, og som går videre end den beskyttelse, som stærk kundeautentifikation giver i forbindelse med betalingstransaktioner, herunder transaktioner, der involverer betalingsinitieringstjenester.

(101) EBA bør udarbejde udkast til reguleringsmæssige tekniske standarder for de specifikke tekniske krav vedrørende mekanismer til overvågning af transaktioner. Sådanne krav bør bygge på merværdien af miljømæssige og adfærdsmæssige karakteristika i forbindelse med betalingstjenestebrugerens betalingsvaner.

...

(103) Svig i forbindelse med kreditoverførsler er i sagens natur tilpænsdygtig og omfatter en åben mangfoldighed af praksisser og teknikker, herunder tyveri af autentifikationsoplysninger, manipulation af fakturaer og social manipulation. For at kunne forhindre stadig nye former for svig bør overvågningen af transaktioner derfor løbende forbedres, idet der gøres fuld brug af teknologi såsom kunstig intelligens. Ofte har en betalingstjenesteudbyder ikke det fulde billede af alle komponenter, der kan føre til rettidig afsløring af svig. Det kan dog gøres mere effektivt med en større mængde oplysninger om potentielt svigagtige aktiviteter fra andre betalingstjenesteudbydere. Det bør derfor være muligt at udveksle alle relevante oplysninger mellem betalingstjenesteudbydere. For bedre at afsløre svigagtige betalingstransaktioner og beskytte deres kunder bør betalingstjenesteudbydere med henblik på overvågning af transaktioner gøre brug af data om betalingssvig, der deles af andre betalingstjenesteudbydere på multilateralt grundlag såsom særlige IT-platforme baseret på ordninger for udveksling af oplysninger. For at forbedre beskyttelsen af betalere mod svig i forbindelse med kreditoverførsler bør betalingstjenesteudbydere kunne forlade sig på så omfattende og ajourførte oplysninger som muligt, navnlig ved i fællesskab at anvende oplysninger om entydige identifikationskoder, manipulationsteknikker og andre omstændigheder i forbindelse med svigagtige kreditoverførsler, der identificeres individuelt af hver enkelt betalingstjenesteudbyder. Inden betalingstjenesteudbydere indgår en aftale om udveksling af oplysninger, bør de foretage en konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med artikel 35 i forordning (EU) 2016/679.

...

(106) Betalingssvindel bliver stadig mere sofistikeret, idet svindlere anvender manipulerende og impersonerende teknikker, som det er vanskeligt for brugerne af betalingstjenester at opdage uden en tilstrækkelig grad af bevidsthed og information om svig. Betalingstjenesteudbydere kan spille en vigtig rolle med hensyn til at styrke forebyggelsen af svig ved regelmæssigt at tage alle nødvendige initiativer for at øge deres betalingstjenestebrugeres forståelse af og bevidsthed om de risici og tendenser, der er forbundet med betalingssvig. Betalingstjenesteudbydere bør navnlig gennemføre passende oplysningsprogrammer og kampanjer om tendenser og risici for svig rettet mod kunder og ansatte hos betalingstjenesteudbydere med henblik på at hjælpe kunderne med at forstå, at de er ofre for et forsøg på svig. Betalingstjenesteudbydere bør via forskellige medier give deres forbrugere tilpassede oplysninger om svig, give dem klare budskaber og advarsler og hjælpe dem med at reagere korrekt, når de udsættes for potentielt svigagtige situationer. EBA bør udarbejde retningslinjer for de forskellige typer programmer, som betalingstjenesteudbydere skal udvikle vedrørende risici for

betalingssvindel, under hensyntagen til den konstant skiftende karakter af de risici, der er forbundet med svig.

...

Artikel 59

Betalingstjenesteudbyderens ansvar for svig i form af at udgive sig for en anden

1. Hvis en bruger af betalingstjenester, som er en forbruger, er blevet manipuleret af en tredjepart, der foregiver at være ansat hos forbrugers udbyder af betalingstjenester ved ulovlig brug af den pågældende betalingstjenesteudbyders navn eller emailadresse eller telefonnummer, og denne manipulation har givet anledning til efterfølgende svigagtige autoriserede betalingstransaktioner, skal udbyderen af betalingstjenester tilbagebetale forbrugeren det fulde beløb for den svigagtige autoriserede betalingstransaktion, forudsat at forbrugeren straks har indberettet svigen til politiet og underrettet sin betalingstjenesteudbyder.
2. Senest 10 arbejdsdage efter at have konstateret eller være blevet underrettet om den svigagtige autoriserede betalingstransaktion skal betalingstjenesteudbyderen gøre et af følgende:
 - a) refundere forbrugeren beløbet for den svigagtige autoriserede betalingstransaktion
 - b) hvis udbyderen af betalingstjenester har rimelig grund til at formode, at forbrugeren har begået svig eller grov uagtsomhed, give en begrundelse for at afslå tilbagebetaling og oplyse forbrugeren om, hvilke organer forbrugeren kan henvende sig til i overensstemmelse med artikel 90, 91, 93, 94 og 95, hvis forbrugeren ikke accepterer den anførte begrundelse.
3. Stk. 1 finder ikke anvendelse, hvis forbrugeren har handlet svigagtigt eller groft uagtsomt.
4. Det påhviler forbrugers betalingstjenesteudbyder at bevise, at forbrugeren har handlet svigagtigt eller groft uagtsomt.
5. Når udbydere af elektroniske kommunikationstjenester underrettes af en betalingstjenesteudbyder om forekomsten af den type svig, der er omhandlet i stk. 1, arbejder de tæt sammen med betalingstjenesteudbydere og handler hurtigt for at sikre, at der er truffet passende organisatoriske og tekniske foranstaltninger til at beskytte kommunikationssikkerheden og -fortroligheden i overensstemmelse med direktiv 2002/58/EF, herunder med hensyn til opkaldsnummeridentifikation og e-postadresse."

Anbringender

Parterne har i det væsentlige procederet i overensstemmelse med, hvad der fremgår af deres påstandsdokumenter for landsretten.

A har herved anført følgende i sit påstandsdokument af 9. september 2026 (henvisninger til ekstrakt og materialesamling samt overskriftsnummerering udeladt):

" ...

Nordea hæfter efter betalingslovens §§ 82, 99 og 100

Bemærkninger til Det finansielle ankenævns praksis

Det centrale spørgsmål efter betalingsloven er, om der består en afgørende forskel i forbrugerens retsstilling mellem tilfælde, hvor forbrugeren som led i telefonsvindlen manipuleres til selv at foretage en overførsel til en „sikker konto“, og tilfælde, hvor forbrugeren ved et tilsvarende manipulerende telefonopkald i stedet forledes til at udlevere kort- eller kontoplysninger til svindlerne. Det finansielle ankenævns praksis fører til, at bankerne kun hæfter i sidstnævnte tilfælde.

Det finansielle ankenævn traf første gang afgørelse om "safe account fraud" i 2021, og nævnets praksis om "safe account fraud" adskiller sig fra nævnets øvrige praksis om betalingsmisbrug i forbindelse med netbankoverførsler. I andre tilfælde, hvor en forbruger kontaktes af en tredjepart, og hvor der efter manipulation sker overførsel af penge fra kundens konto til svindlerens konto, har nævnet fastslået, at pengeinstituttet hæfter. Dette omfatter bl.a. (1) tilfælde, hvor kunden videregiver NemID-oplysninger til svindlere, som foretager overførslen via netbank, eller (2) klassiske "phishing"-tilfælde, hvor kunden modtager et link og bliver manipuleret til at indtaste kontoplysninger og foretage den for transaktionen afgørende godkendelse i nøgleappen.

Det finansielle ankenævns daværende formand, fhv. højesteretsdommer Vibeke Rønne, har anført som begrundelse for denne sondring i nævnets praksis, at "safe account fraud" svarer til en situation, hvor kunden afleverer kontanter til en person, der viser sig at være svindler (...). Dette bestrides. Når overførsler sker via netbank, er der ikke tale om et topartsforhold, men om et aftalebaseret trepartsforhold, hvor Nordea som betalingsformidler indtager rollen som mellemlid, der må påtage sig risikoen for at udfylde denne rolle, bl.a. ved at blive mødt med ugyldighedsindsigelser eller ved at blive erstatningsansvarlig for ikke at tilbyde den sikkerhed, som bør forventes. På den baggrund beror Det finansielle ankenævns retlige vurdering i sager om "safe account fraud" på en fejlagtig retsanvendelse.

Det netop anførte understøttes af, at retsstillingen er den modsatte i andre lande. Det norske finansielle ankenævn, Finansklagenemnda, har ikke fundet grundlag for at sondre mellem "safe account fraud" og anden netbanksvindel, og i begge tilfælde hæfter pengeinstituttet derfor.

Betalingsloven stiller krav om samtykke

Efter betalingslovens § 99, stk. 1, hæfter udbyderen (pengeinstituttet) for tab som følge af uautoriserede betalingstransaktioner, og betalingslovens § 100 regulerer tabsfordelingen mellem betaler (kunden) og udbyder, hvis der sker uberettiget anvendelse af en betalingstjeneste. Om brug af en betalingstjeneste er uberettiget eller ej efter betalingslovens § 100, afgøres efter lovens § 82, stk. 1. Af bestemmelsen fremgår, at en betalingstransaktion kun er "autoriseret", hvis betaleren har meddelt

samtykke til at gennemføre transaktionen. Har betaleren ikke meddelt gyldigt samtykke, er transaktionen "uautoriseret", jf. § 82, stk. 1, 3. pkt., og i så fald regulerer § 100 tabsfordelingen. Det klare udgangspunkt for bestemmelsen er, at udbyderen skal bære tabet, hvis en betalingstjeneste misbruges. Kun hvis der foreligger særlige omstændigheder, hæfter betaleren for (en del af) tabet, jf. betalingslovens § 100, stk. 2-5.

Nordea har anført, at sagen angår en "autoriseret" transaktion ud fra den betragtning, at "samtykke" efter betalingslovens § 82 må forstås som "den tekniske godkendelse af en betaling". Nordeas synspunkt synes at være, at de almindelige gyldighedskrav og retsvirkninger af det juridiske begreb "samtykke" ikke finder anvendelse på samtykkebegrebet i betalingsloven. Konsekvensen af Nordeas synspunkt er derfor også, at en "teknisk godkendelse" ikke kan blive mødt med aftalerettens almindelige ugyldighedsindsigelser om fx svig eller tvang. Hvis dette var tilfældet, ville betalingsloven ikke sikre det hensyn til forbrugerbeskyttelse, som er hele lovens grundlag. Der er ingen støtte i forarbejderne for, at lovgiver har haft ønske om at indsnævre den typiske betydning begrebet "samtykke" og de hertil hørende retsvirkninger.

A gør gældende, at begrebet "samtykke" i betalingslovens § 82 forudsætter et gyldigt samtykke. En følge heraf er, at spørgsmålet om hæftelse ikke blot beror på, om kunden rent praktisk har gennemført transaktionen i sin teknikalitet, men om kunden har givet et gyldigt samtykke til den konkrete transaktion. Da Det finansielle ankenævn i vurderingen af betalingsloven har lagt vægt på det rent tekniske forhold, hvem der rent praktisk gennemførte overførslen, er det As opfattelse, at nævnets regelanvendelse er forkert.

Det er ubestridt, at A blev udsat for telefonisk manipulation og handlede i den tro, at hun skulle redde sit indestående. På den baggrund har hun ikke givet gyldigt samtykke til de konkrete betalingstransaktioner til ukendte tredjemænd, som faktisk fandt sted. Nordea hæfter derfor efter betalingslovens §§ 82, jf. 99, stk. 1 og 100, stk. 1, for As tab, subsidiært for det fulde tab med fradrag for de begrænsede beløb på 375 kr. eller 8.000 kr., som forbrugeren kan hæfte for efter betalingslovens § 100, stk. 3 eller 4.

Lovens formål

Nordea har anført som hovedsynspunkt, at "betalingslovens §§ 89 og 100 gør endeligt op med ansvarsfordelingen mellem pengeinstitutter og deres kunder", og "at lovgiver ikke har efterladt rum til, at domstolene kan indføre ansvar for pengeinstitutter i situationer, hvor kunden selv har overført beløbet." Dette bestrides.

Når det fremgår af lovforarbejderne, at betalingsloven gør endeligt op med ansvarsfordelingen, er udtrykket anvendt i forbrugernes og ikke betalingsformidlernes (herunder bankernes) favør. Det er således korrekt, at betalingslovens § 100 gør op med almindelige erstatningsretlige regler, hvad angår *forbrugerens* hæftelse og ansvar i forhold til udbyderen. Dette betyder, at forbrugeren ikke kan hæfte i videre udstrækning,

end det fremgår af betalingslovens § 100. For så vidt angår udbyderens hæftelse, er betalingsloven derimod en minimumsbeskyttelse af forbrugerne, og rækkevidden af denne beskyttelse fastsættes af domstolene på baggrund af almindelig lovfortolkning.

Konsekvensen af Nordeas synspunkt er en sontring, hvor det gør en helt afgørende forskel for forbrugerens retsstilling, om forbrugeren selv har initieret misbrugstransaktionen på grundlag af tredjemands bedrageriske opkald, eller om forbrugeren under et helt tilsvarende opkald har videregivet sine oplysninger til en tredjemand, som herefter initierer transaktionen. A gør gældende, at der ikke er grundlag i lovforarbejderne for denne sontring, og at en sådan – for forbrugeren helt vilkårlig – retsstilling, er i strid med betalingslovens formål, som er at sikre forbrugerbeskyttelse i tilfælde af misbrug.

Lovens forarbejder

Betalingslovens hæftelsesregler er en videreførelse af de regler, som fremgik af lovens forgængere i form af betalingstjenesteloven (lbkg 2015 613), betalingsmiddeloven (lbkg 2008 259) og betalingskortloven (lbkg 1994 811). I vid udstrækning kan lovforarbejder og praksis vedrørende de forudgående love anvendes ved fortolkning af betalingsloven. Siden den oprindelige betalingskortlovs indførelse har hæftelsesreglernes formål været, at bankerne skal sikre kunden mod ruinering og velfærdstab i tilfælde af misbrug. Af forarbejderne til betalingskortloven fremgik det bl.a. (LFF 1993-12-16 nr. L 133, sp. 5343):

"Betalingskortloven er baseret på bærende principper om, at systemerne skal indrettes således, at der sikredes brugerne 'overskuelighed', 'frivillighed' og 'beskyttelse mod misbrug'.
[...]

I den forudgående betænkning nr. 1255/1993, s. 46 fremgik det bl.a.:

"Misbrug omfatter ikke blot beskyttelse imod tilsigtet misbrug, men tillige beskyttelse imod urimelighed i bred forstand for brugerne, som fx for ringe sikkerheds- og korrektionsprocedurer... Udvalget er enig om, at brugere af home-banking og home-shopping systemer har et tilsvarende behov for beskyttelse imod misbrug"

Af forarbejderne til lov om betalingsmidler fremgik bl.a. (LFF 1999-10.27 nr. 63, sp. 1558):

"Hovedsigtet med lovens regulering er således, at der udbydes sikre og velfungerende betalingsmidler, som dels kan anvendes uden større risici for økonomiske tab som følge af misbrug og fejl eller kompromittering af fortrolige oplysninger, og som dels er indrettet og fungerer hensigtsmæssigt og driftssikkert. Lovens bestemmelser skal endvidere medvirke til at give brugerne og betalingsmodtagerne en rimelig retsstilling ..."

Af forarbejderne til betalingstjenesteloven (LFF 2009-01-28 nr. 119) fremgik det endvidere bl.a.:

”Der er i loven bestemmelser om hæftelse, som sikrer, at brugerne ikke lider et urimeligt stort tab, hvis betalingsmidlet for eksempel bliver stjålet og derefter misbrugt.”

På intet tidspunkt har lovgiver fremhævet, at den tekniske metode for svindleres bedrageri – eller kundens konkrete rolle i forbindelse med tredjemands bedrageri – skal have betydning for kundens retsstilling. Tværtimod viser forarbejderne og ansvarsfordelingen i § 100, at hensigten bag loven er at tillægge forbrugerbeskyttelsen afgørende vægt, og kun hvis der foreligger særlige omstændigheder, skal forbrugeren hæfte for en helt begrænset del af tabet, jf. § 100, stk. 3 og 4. På denne vis afvejer reglerne styrkeforholdet mellem bankerne, som har mulighed for at indrette deres systemer og pulverisere deres tab, og den borger, for hvem misbrug kan være velfærdstruende.

I takt med den teknologiske udvikling er misbrugstruslen ændret fra primært at angå bankrøverier, til skade for pengeinstitutterne og deres medarbejdere, til udelukkende at omfatte netsvindler i stadigt nye former, til skade for kunderne. Denne udvikling illustrerer, at lovgiver ikke har kunnet forudse enhver ny svindelform ved lovens formulering. Dette ændrer ikke på, at også nye svindelformer udgør kerneområdet for hæftelsesreglernes formål, som angår ”misbrug”. På denne baggrund bør det ikke være afgørende for forbrugernes retsstilling, om tredjemand har ”anvendt” betalingssystemet i den forstand, at tredjemand selv har interageret med systemer ved at foretage overførslen, eller om tredjemand på anden måde har ”anvendt” systemet ved at udnytte systemets sikkerhedsmæssige huller, fx gennem bedrageriske telefonopkald. Dette understøttes direkte af de specielle bemærkninger til 2017-lovændringen, som viser, at lovens ordlyd skal tilpasses de svindeltyper, som måtte udvikle sig. Af lovbemærkningerne fremgår, at forbrugeren på grund af manglende forsæt til den uberettigede anvendelse ikke hæfter efter § 100, stk. 4 og 5 i forbindelse med ”phishing”, selvom lovens ordlyd umiddelbart kan tale i anden retning. Lovgiver anførte i lovforarbejderne bl.a. (LFF 2017 157, s. 169):

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

...

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

til andre, eksempelvis i forbindelse med phishing, hæfter betaler ikke efter forslaget til stk. 5, idet betaler ikke overdrog den personlige sikkerhedsforanstaltning med forsæt til at der skal foretages den uberettigede anvendelse."

I 2017, hvor hæftelsesreglerne senest blev ændret, var "safe account"-svindel ikke kendt, og derfor adresserer forarbejderne ikke denne svindeltype. Men 2017-lovforarbejderne viser, at det retlige blik ikke skal rettes mod, hvordan misbruget er sket i sin teknikalitet, herunder om overførslen er muliggjort ved overdragelse af nøglekort eller ved betalerens egne overførsler. Det afgørende er derimod, om betaleren havde *forsæt* eller *vilje* til, at det uberettigede element fandt sted. På samme måde som en bruger, der udsættes for svindel ved "phising", ikke har forsæt til den uberettigede anvendelse, har den kunde, der udsættes for "safe account fraud", hverken forsæt eller vilje til det uberettigede element i form af overførsel af hele sit indestående til ukendte svindlere. På denne baggrund bør betalingslovens § 100 i det mindste anvendes på samme måde ved "safe account fraud" og "phising". Nordea hæfter derfor efter lovens § 82, jf. § 100, stk. 1 og 3.

Forholdet til EU-retten

Den gældende betalingslov implementerer 2. betalingstjenestedirektiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked. Nordea har fremhævet, at Europa-Parlamentet og Rådet den 28. juni 2023 har fremsat og førstebehandlet forslag til Forordning om betalingstjenester, hvoraf det fremgår direkte af en ny artikel 59, at banken hæfter i tilfælde af "safe account fraud". Nordea har benyttet dette ændringsforslag til at fremføre, at konsekvensen af forslaget er, at der ikke var grundlag for at placere et ansvar hos pengeinstitutterne i tilfælde af "safe account fraud" efter det gældende 2. betalingstjenestedirektiv (EU) 2015/2366 af 25. november 2014 (...). Dette bestrides. Det fremgår direkte af betragtning (3) og (4) til forordningsforslaget, at 2. betalingstjenestedirektivs mål også omfattede "safe account fraud":

... [citeret ovenfor i afsnittet om retsgrundlaget]

Af betragtning (79) til forordningsforslaget fremgår det endvidere:

... [citeret ovenfor i afsnittet om retsgrundlaget]

Som forordningsforslaget viser, er den fortolkning af begreberne "autoriseret" og "uautoriseret", som Nordea lægger vægt på, ikke relevant ved nye svindeltyper såsom "safe account fraud", hvor sondringen udviskes. Forslaget viser samtidig, at hensigten med disse begreber ikke har været at begrænse bankernes hæftelse i tilfælde, hvor forbrugeren selv foretager den tekniske godkendelse. Tværtimod viser forslaget, at de betingelser, hvorunder kunden godkendte en transaktion, netop skal tillægges vægt, og at direktivets mål også i disse tilfælde er hæftelse for bankerne.

Herudover fremgår det direkte af lovforarbejderne fra 2017, at den danske retsstilling for bankers hæftelse på flere punkter rækker videre end de forpligtelser, som følger af EU-retten, og at hensigten netop er en videregående beskyttelse. Det centrale er derfor, hvilken hensigt den danske lovgiver har udtrykt gennem årene i relation til betalingslovens formål.

Nordea hæfter efter aftalelovens § 30 på grund af tredjemands svig

Nordea hæfter for As tab efter aftalelovens § 30, stk. 1, fordi Nordea, der på tidspunktet for hændelsen havde kendskab til både "safe account fraud" og As betalingsmønstre, burde have indset, at overførslerne var resultatet af svig fra tredjemand. A har ikke afgivet en viljeserklæring, som skaber retsvirkninger, og det burde Nordea have vidst.

Svig er en svag ugyldighedsindsigelse, som alene kan gøres gældende, når adressaten er i ond tro. Betingelserne for Nordeas burde-viden må svare til de krav, som domstolene ville stille til en medarbejder, som modtog tilsvarende betalingsinstruktioner i den fysiske verden. Nordea kan ikke undgå en svigsindsigelse efter aftalelovens § 30 ved at indrette sig med et fuldautomatisk betalingssystem i stedet for manuel håndtering af overførsler foretaget af en medarbejder, som pengetransaktioner tidligere var baseret på. Det forhold i øvrigt, at oplysninger i et it-system kan påføre indehaveren ond tro ("systemisk ond tro"), er fastslået af bl.a. Högsta Domstolen i dom af 1. juli 2025.

I UfR 2022.414 H om et par, som var blevet narret til at udlevere NemID, udtalte Højesteret, at parret ikke hæftede for lånet, og at vurderingen af, om parret skulle anses for "aftaleretligt forpligtet", skulle basere sig på en "konkret vurdering af det samlede hændelsesforløb". A gør gældende, at den samme vurdering bør anvendes denne sag. I forbindelse med denne helhedsvurdering bør navnlig følgende tillægges vægt:

Bevisbyrde

Nordea bærer bevisbyrden for, at Nordea ikke var i ond tro.

Nordea gjorde det under sagens forberedelse for byretten vanskeligt for A at fremlægge beviser for, at Nordeas systemer kunne og burde have reageret på de retsstridige hævninger på en måde, der effektivt havde hindret dem. As processuelle opfordringer, bl.a. om hvilke procedurer, kundeorienteringer, kontroller, overvågningsmekanismer mv., Nordea havde foretaget overfor "safe account fraud", besvarede Nordea med henvisning til navnlig, at forholdene ville blive belyst af Nordeas vidner. Da hovedforhandlingen i byretten nærmede sig, begærede Nordea dørlukning, angiveligt fordi Nordeas vidner ville udtale sig om sikkerhedsfølsomme oplysninger, som offentligheden ikke måtte få kendskab til. Denne begæring efterkom byretten, trods As protest. Under forklaringerne viste det sig, at Nordeas vidner ikke udtalte sig om sikkerhedsfølsomme oplysninger, at der ifølge vidnerne ikke var

udløst nogen egentlige alarmer til den relevante afdeling i den konkrete sag, ligesom Nordeas vidnes svar om tidspunktet for Nordeas kendskab til "safe account fraud" var ukorrekt.

I en forbrugersag, hvor en kunde har mistet hele sit indestående, er det i særdeleshed opsigtsvækkende, at oplysningen fra Nordeas vidner om, at Nordea først fik kendskab til "safe account fraud" omkring sommeren 2022, kort tid før A blev svindlet, var notorisk ukorrekt. For landsretten har A fremlagt dokumentation for, at Nordea var fuldt ud vidende om "safe account fraud" lang tid før det tidspunkt, hvor A blev svindlet.

Med denne viden, som foreligger for landsretten, om vidnernes forklaringer, bør bevisbyrden skifte til skade for Nordea, således at Nordea bør godtgøre, at Nordea ikke var i ond tro, da A blev udsat for netop de karakteristika, som Nordea vidste var kendetegnet for "safe account fraud".

Det bemærkes herved, at tidspunktet for Nordeas kendskab til denne type svindel er nævnt direkte i byrettens præmisser, og forholdet har således haft betydning for byrettens vurdering af culpaspørgsmålet, ligesom det bør have betydning for ond tros-vurderingen efter aftalelovens § 30, stk. 1. I begge henseender er netop Nordeas viden af afgørende betydning.

A reagerede straks

Ved vurderingen af, om A skal forpligtes aftaleretligt, må det tillægges vægt, at hun reagerede straks, jf. også U 2022.414 H (...). A indgav sin indsigelse allerede om formiddagen den 23. august 2022, så snart misbruget stod klart.

Nordea havde indgående viden om As betalingsmønstre

A har som enlig pensionist foretaget få betalinger af mindre beløb, som er præget af en fast rutine, og hun gør minimal brug af sin netbank, hvilket er ubestridt. På grundlag af sit indgående kendskab til As kundeadfærd gennem mere end 50 år, burde Nordea have reageret på de helt atypiske betalingsmønstre, som fandt sted den 22. og 23. august 2022.

Nordea havde indgående kendskab til "safe account fraud" i august 2022

Det forhold, at Nordea havde burde-viden om, at A var udsat for svindel, understøttes som anført af, at Nordea på svindeltidspunktet var fuldt ud bekendt med "safe account fraud" og den for denne svindelform kendetegnende fremgangsmåde:

- Det finansielle ankenævn traf den første afgørelse om "safe account fraud" allerede den 9. november 2021 (...) i en sag, hvor Nordea var indklaget, og hvor det bedrageriske telefonopkald var

foretaget allerede den 28. oktober 2020. I august 2022, hvor A blev udsat for svindel, var Nordea endvidere indklaget i 9 andre sager, hvilket langt oversteg antallet for andre institutter.

- Offentligt tilgængelige oplysninger viser, at "safe account fraud" var velkendt og velbeskrevet i den finansielle sektor lang tid før august 2022, og konkurrerende banker foretog aktive tiltag og advarede sine kunder direkte mod denne form for misbrug.
- Nordeas egen hjemmeside indeholdt allerede den 28. september 2021 oplysninger, som viste, at Nordea var bekendt med svindlernes fremgangsmåde ved "safe account fraud" (.). Disse oplysninger fremgik af en underside, som var tilgængelig via et link allernederst på Nordeas hjemmeside. Oplysningerne var derfor ikke synlige for den almindelige kunde i de sammenhænge, hvor en advarsel er relevant. Det bemærkes, at de fleste kunder benytter en app på mobiltelefonen til netbankforretninger, hvor disse oplysninger ikke fremtræder.
- Ifølge sagens oplysninger led Nordeas kunder allerede i 2021 tab for 6 millioner kr. som følge af "safe account fraud". Dette tal steg til 40 millioner kr. i 2022, hvor 900 kunder i Nordea blev udsat for "safe account fraud".

Nordea havde burde viden (ond tro)

Det fremstår usandsynligt, at A har haft til hensigt i de sene aftentimer pludselig at overføre hele sit indestående ved 9 på hinanden følgende overførsler til ukendte konti. Enhver bankansat, der som Nordea havde kendskab til fremgangsmåden ved "safe account fraud", ville have indset, at A måtte være udsat for svig. Sagens oplysninger viser endvidere, at Nordeas system krævede en "second channel confirmation" i forbindelse med alle 9 transaktioner. På den baggrund identificerede Nordeas system alle ni transaktioner som atypiske, hvilket taler for ond tro. Sagens oplysninger viser også, at bankssystemer, som evaluerer kundernes transaktionsmønstre og stopper unormale transaktioner er gængs, og Nordea burde således også være i stand til at opdage de helt atypiske transaktioner, som fandt sted på As konti. Efter en konkret vurdering af det samlede hændelsesforløb burde Nordea således have indset, at de 9 overførsler hver især og samlet var en følge af svig. På denne baggrund er As viljeerklæringer ugyldige, og Nordea hæfter for tabet, jf. aftalelovens § 30, stk. 1.

Nordea hæfter på grundlag af aftalelovens §§ 36 og 38 c

A gør gældende som subsidiaer ugyldighedsgrund, at hun ved at indgå netbankaftalen med Nordea er blevet påført en urimelig risiko for et helt uventet og betydeligt tab svarende til hendes likvide formue. En sådan uventet retsvirkning af den indgåede aftale er uforudset, uproportional og dermed urimelig for A som forbruger. De retsvirkninger, som følger af aftalen må

derfor i alle tilfælde lempes i medfør af aftalelovens §§ 36 og 38 c med den konsekvens, at Nordea hæfter for As tab.

Det er Nordea, der har designet det betalingssystem, som A benyttede, og Nordea høster rationalitetsgevinsterne ved det. Det derfor vil være urimeligt, hvis en følge af As aftale med Nordea – hvor hun ikke har kunnet fravælge netbanksystemet – er, at Nordea kan påberåbe sig en betalingsordre, som ubestridt og tydeligt for enhver iagttager ikke dækkes af As hensigt.

Når svindlere finder huller i bankens sikkerhedssystem ved at narre kunderne af en påstået bankmedarbejder til at overføre penge til en sikker konto, er det alene Nordea, som er i stand til at forebygge dette – ikke bankkunden. Det vil derfor være urimeligt, jf. aftalelovens §§ 36 og 38 c, at pålægge forbrugeren ansvaret.

Nordea er erstatningsansvarlig

A gør endelig gældende, at Nordea er erstatningsansvarlig for As fulde tab efter dansk rets almindelige regler om erstatning i kontrakt.

For det første er Nordea underlagt et professionsansvar. Nordeas virksomhed kræver en særlig fagkyndighed, herunder med offentligretlig tilladelse på et område, hvor kunderne betror deres formue til Nordea, og Nordea udbyder det betalingssystem, som kunderne er nødsaget til at anvende. Hvis Nordeas sikkerhedssystemer ikke er garderet mod de svindelformer, som er aktuelt forekommende, og som Nordea er nærmest til at kende, påhviler risikoen herfor Nordea (...). Det er Nordeas ansvar at indrette sine systemer på en måde, som ikke indebærer en nærliggende risiko for tab hos kunden, jf. bl.a. U.1968.84/2H, U.1983.866/2H, U.1983.714/2H, U.1996.200/2H, U.1999.1821/2H og U.2000.1779 H (...), hvor erstatningsansvaret påhvilede den, som ved sin tekniske og økonomiske planlægning havde mulighed for at tage risikoen for tab i betragtning. Nordea har både kunnet indregne den statistisk set uundgåelige risiko for tab i sin forretningsmodel og træffe de nødvendige foranstaltninger for at imødegå tab.

For det andet er Nordea underlagt offentligretlige regler, som Nordeas kunder kan forvente vil blive overholdt som led i aftaleforholdet. I medfør af § 8, stk. 2, i bekendtgørelsen om god skik for finansielle virksomheder, er Nordea forpligtet til at yde rådgivning "hvis kunden anmoder herom", men også "... af egen drift yde rådgivning ... hvor omstændighederne tilsiger, at der er behov herfor". Hvis disse regler ikke iagttages, hvilket beror på en konkret vurdering, ifalder Nordea erstatningsansvar, jf. §§ 43 og 43 a i lov om finansiell virksomhed.

Bevisbyrde

I rådgivningssituationer, hvor omstændighederne tilsiger, at der er et særligt behov for at rådgive kunden, vendes bevisbyrden, så den finansielle virksomhed har bevisbyrden for, at virksomheden ikke har handlet culpøst. For så vidt angår netop "safe account fraud" er der tale om en svindeltype, hvor kunden risikerer at tabe hele sit indestående, og hvor Nordea har været af den opfattelse – som sagen viser – at kunden selv hæfter for tabet, som altså kan være velfærdstruende. På denne baggrund tilsiger de konkrete omstændigheder efter As opfattelse i særlig grad, at Nordea skulle yde rådgivning og træffe nødvendige forholdsregler for at sikre A og andre kunder imod risikoen for tab ved "safe account fraud", hvilket ikke skete.

For så vidt angår Nordeas professionsansvar, gør A tilsvarende gældende, at det i en sag som den foreliggende, hvor en forbruger har tabt hele sit indestående i forbindelse med brug af Nordeas betalingssystemer, må påhvile Nordea som den professionelle at godtgøre, at Nordeas betalingssystemer havde sikkerhedsforanstaltninger som på relevant vis var egnede til at imødegå "safe account fraud", navnlig om så store – for kunden atypiske – overførsler udført på døgnets ydertimer, som sagen angår. Denne bevisbyrde har Nordea ikke løftet. Tværtimod viser sagens oplysninger, at Nordea har undladt at tage adækvate skridt mod den risiko, som "safe account fraud" har frembudt for kunderne.

Nordea har undladt at opfylde sin handlepligt

As tab er en direkte følge af, at Nordea ikke havde egnede kontrolforanstaltninger rettet mod "safe account fraud" på tidspunktet for misbruget, og i øvrigt at Nordea undlod straks at tilbageføre beløbene, da A mødte op i Nordeas fysiske afdeling om formiddagen den 23. august 2022. Kravet om årsagsforbindelse og adækvans er derfor opfyldt. Eftersom A straks anmeldte forholdet, er der ikke grundlag for overvejelser om egen skyld. Til de forholdsregler, som Nordea har påberåbt sig bemærkes:

Nordea har ikke rådgivet A om "safe account fraud"

Sagens oplysninger viser, at Nordea ikke rådgav A om risikoen for "safe account fraud" før hændelsen i 2022. A blev ikke under overførslerne mødt med advarsler – fx konkrete SMS-advarsler rettet mod telefonsvinde eller pop-up vinduer, der var aktive uden for bankens åbningstid – eller med andre restriktioner, som var egnede til at afværge eller forsinke overførslerne.

Nordea har anført under sagen, at Nordea i det halve år op til august 2022 løbende havde advarsler på bl.a. netbank. Dette er udokumenteret. Der er ikke fremlagt nogen dokumentation til støtte for, at Nordea havde løbende og relevante advarsler i forbindelse med brug af netbank, herunder ved brug af netbank via app i mobilversioner, eller at A på anden måde blev advaret om risikoen for "safe account fraud". Det fremgår derimod af sagen, at Nordea efterfølgende begyndte at give kunderne sådanne konkrete advarsler.

Nordeas tiltag var uvirksomme i forhold til "safe account fraud"

Det er ubestridt, at Nordeas system krævede en "second channel confirmation" i forbindelse med alle 9 transaktioner. På den baggrund identificerede Nordeas system alle ni transaktioner som atypiske. På tidspunktet for hændelsen udløste denne identifikation fra Nordeas side alene denne "second channel confirmation", som bestod i en generaliseret SMS, hvor kunden blev bedt om at bekræfte, at overførslerne ønskedes gennemført.

En sådan SMS er en egnet kontrolforanstaltning i tilfælde, hvor kunden ikke er klar over, at overførslen finder sted, fx fordi tredjemand forsøger at foretage overførsler fra kundens konto, som kunden ikke har kendskab til, og hvor kunden derfor får mulighed for at bremse transaktionen. Det forholder sig modsat ved "safe account fraud", hvor kunden er i vildfarelse om overførslens modtager. I sådanne tilfælde er en *generaliseret* SMS-bekræftelse efter sin karakter ikke en egnet kontrolforanstaltning. Dette understøttes af forklaringen i byretten af Strategic Project Leader hos Nordea, Lucja Wägander:

"Ved "second channel confirmation" rækker de ud til kunden på en effektiv måde, som stopper megen svindel, og de er nødt til at stole på kunden, når kunden ønsker at gennemføre overførslen".

Problemet er, at kunden ikke har noget ønske om at gennemføre den overførsel, som faktisk finder sted. Eftersom det karakteristiske ved "safe account fraud" netop er, at kunden bliver foranlediget til at tro, at overførslen sker til "en sikker konto", og at overførslen er nødvendig for, at kunden ikke mister sine midler, er kunden direkte ansporet til at bekræfte en sådan SMS. Det forhold, at As overførsler blev gennemført med "to-faktor-autentifikation" med brug af NemID og ved "second channel confirmation", er således irrelevante i relation til "safe account fraud". Sagens oplysninger viser da også, at Nordea efterfølgende har ændret praksis for "second channel confirmation", idet Nordea nu anvender en *konkretiseret* SMS-advarsel, som omfatter risikoen for telefonsvindel.

Foruden "second channel confirmation" havde Nordea ifølge forklaringerne i byretten adfærdsmonitorering i realtid for bl.a. privatkunder i netbank, og Nordeas system kunne udløse en alarm, som ville blive håndteret af et team af medarbejdere, som arbejdede på hverdage fra kl. 08.00 til kl. 16.00. Hvis der udløstes en alarm uden for afdelingens arbejdstid, ville alarmen først blive håndteret dagen efter. Selvom Nordeas eget system altså identificerede alle 9 overførsler i sagen som atypiske og udløste krav om "second channel confirmation", fremgår det af forklaringerne for byretten, at der ikke blev udløst en alarm til de medarbejdere, der håndterer svindelsager, og som i øvrigt først mødte på arbejde næste dag.

Samlet set viser sagens oplysninger, at selvom Nordea på den ene side identificerede overførslerne som atypiske, blev dette ikke fulgt op af foranstaltninger, som ville kunne bremse eller forhindre overførslerne.

De foranstaltninger, som Nordea fremhæver i sagen, er efter deres karakter ikke egnede til at imødegå det misbrug, som A blev udsat for. Eftersom Nordea har ansvaret for systemets indretning, bærer Nordea også ansvaret for, at A ikke blev advaret om den risiko, som Nordea var fuldt ud bekendt med, og som Nordea efterfølgende har truffet forholdsregler overfor.

Nordea har undladt at reagere ved ikke straks at tilbageføre beløb

Sagens oplysninger viser, at 7 af de 9 overførsler skete til 3 konti i Nordea. Uanset heraf har Nordea afvist at kunne tilbageføre noget beløb til A. A gør gældende, at Nordeas afvisning ikke har støtte i de rent tidsmæssige forhold, da de relevante konti havde betragtelige indeståender i hvert fald den 23. og 24. august 2022

Ifølge Nordeas egne oplysninger kan tilbageførsel ske, hvis betalingsafsenderens pengeinstitut betragter det som økonomisk kriminalitet. Som begrundelse for afvisningen har Nordea anført, at tilbageførsel ikke kunne nås i det konkrete tilfælde. Om de faktiske forhold har Nordea oplyst, at penge i svindelsager typisk flyttes hurtigt, og at Nordeas fraud-afdeling havde oprettet sagen den 23. august 2022 kl. 14:48, og kl. 15.06 havde Nordea givet meddelelse til de banker, som pengene var overført til, hvilket altså i hovedsagen var Nordea selv. Det er imidlertid ikke nok at oprette en sag i løbet af eftermiddagen og herefter afvise muligheden for tilbageførsel. Det bør komme Nordea til skade, at Nordea ikke har dokumenteret nogen egentlige forsøg på tilbageførsel, selvom sagens oplysninger tyder på, at tilbageførsel måtte være mulig.

A gør gældende, at det er ansvarspådragende, at Nordea ikke straks sikrede tilbageførsel ved As henvendelse ved fysisk fremmøde om formiddagen den 23. august 2022 straks efter misbruget den foregående aften. Det påhviler Nordea at have interne processer, som sikrer øjeblikkelig tilbageførsel, så snart kunden henvender sig. Dette gælder i særdeleshed i et tilfælde, hvor en kundes penge overføres af svindlere til Nordeas egne konti, som Nordea har råderet over. Det bemærkes, at den tilbageførsel på DKK 17.707,38, som A har modtaget retur, og som stammer fra svindlen, kom fra Danske Bank. Det forhold, at Danske Bank var i stand til at tilbageføre beløb, har betydning for sagen, da der er tale om samme svindelforhold, hvor svindlerne må antages at have handlet med samme hurtighed i relation til både Nordea og Danske Bank.

Nordea er klart overrepræsenteret i sager ved Det finansielle ankenævn. Nordea er klart overrepræsenteret i sager om "safe account fraud" ved Det finansielle ankenævn. Nordea var således indklaget i mere end 50 % af nævnets sager om "safe account fraud" i 2021-2025 (...). Dette kan ikke forklares med henvisning til Nordeas størrelse, eftersom fx Danske Bank ikke er indklaget i nær samme antal sager. Enten har andre banker langt bedre kontrolforanstaltninger, hvilket sagens oplysninger kan tyde på, eller også har andre banker påtaget sig hæftelsen, ligesom den norske filial af Nordea og andre norske banker

har gjort. Nordea har bevisbyrden for, at denne overrepræsentation ikke skyldtes Nordeas mangelfulde foranstaltninger, og denne bevisbyrde er ikke løftet. Nordeas overrepræsentation understøtter tværtimod, at Nordea har indrettet sin drift på en måde, som har indebåret en nærliggende risiko for tab for Nordeas kunder, og som har været utilstrækkelig set i forhold til andre banker.

BYRETTENS DOM

A forstår byrettens præmisser sådan, at byretten lægger afgørende vægt på, om A har afgivet et gyldigt samtykke til de konkrete overførsler ved viljeserklæringer (i form af påbud), som er bindende. Landsretten bør betragte betalingsloven på samme måde.

Derimod er byrettens vurdering af, om A har afgivet en bindende viljeserklæring til de overførsler, som fandt sted, fejlagtig. Byretten lægger fejlagtigt vægt på, at Nordea havde indført "second channel confirmation" i form af et krav om SMS-bekræftelse ved overførsel af bl.a. højrisikotransaktioner. Eftersom A var i en vildfarelse om, at det var nødvendigt at overføre sit indestående, havde hun incitament til at godkende den SMS, hvilket gerningsmændene også ansporede hende til. På den baggrund er det fejlagtigt, når byretten under henvisning til denne "second channel confirmation" afviser, at Nordea var i ond tro. Den generiske SMS var ikke egnet til at bringe A ud af sin vildfarelse. På den baggrund tjente SMS'en slet ikke som kontrolforanstaltning i relation til "safe account fraud", og den var derfor heller ikke egnet til at bringe Nordea i god tro.

For så vidt angår Nordeas erstatningsansvar, har byretten anvendt den almindelige culparegel ukorrekt ved at afvise culpa med den begrundelse, at der ikke er "fremkommet oplysninger om en branchenorm for indretning af pengeinstitutters overvågning af svindel foretaget via netbank...". Om der foreligger culpa, indebærer en retsanvendelse, som domstolene må foretage ud fra en konkret vurdering af skadessituationen, herunder med relevante risikobetragtninger. Denne stillingtagen kan ikke forvandles til et bevisspørgsmål om, hvorvidt der har foreligget en branchepraksis, navnlig ikke når de enkelte bankers procedurer ikke er kendte. Det brancheforhold, som kan tillægges vægt, er, at andre pengeinstitutter end Nordea slet ikke er repræsenteret i det finansielle ankenævns praksis om "safe account fraud" i samme grad som Nordea.

OM A'S PÅSTAND

As betalingspåstand svarer til hendes reelle tab i form af de 9 overførsler, som sagen angår, med fradrag for 17.707,38 kr., som Danske Bank tilbageførte, og som A derfor har fået retur.

Hvis landsretten ikke giver A medhold i den principale påstand, gøres det gældende, at A bør tilkendes et lavere beløb, som principalt bør være 398.582,62 kr. svarende til retsstillingen efter betalingslovens § 100, stk. 3, eller subsidiært 390.957,62 kr. svarende til den retsstilling,

som følger af betalingslovens § 100, stk. 4, og som er i overensstemmelse med mindretallets opfattelse i Det finansielle ankenævn.

Hvis landsretten ikke er enig i, at Nordea hæfter i overensstemmelse med retsstillingen efter betalingslovens § 100, gør A gældende, at Nordea bør betale 338.217,62 kr. svarende til hendes fulde tab med undtagelse af den første overførsel på 60.740 kr. ud fra den betragtning, at Nordea senest ved den anden overførsel med sikkerhed måtte være i ond tro, jf. aftalelovens § 30, stk. 1.

Hvis landsretten ikke er enig heri, bør Nordea i hvert fald erstatte A for 316.485,00 kr. svarende til de 7 overførsler til konti i Nordea, som Nordea selv havde rådighed over, og som Nordea derfor straks kunne have bremset.

Rentepåstanden er opgjort fra den 5. september 2022, hvor klagen blev indgivet til Det finansielle ankenævn, jf. rentelovens § 3, stk. 4.”

Nordea har heroverfor anført følgende (henvisninger til ekstrakt og materiale-samling samt overskriftnummerering og henvisninger til afsnit udeladt)

” ...

Nordea hæfter ikke i medfør af betalingslovens bestemmelser

Indledning

Det følger af betalingslovens § 99, at udbyderen af en betalingstjeneste hæfter for betalerens tab, hvis tabet er påført som følge af en uautoriseret betalingstransaktion. Hvis tabet er påført ved andres uberettigede anvendelse af et betalingsinstrument, fastlægges ansvarsfordelingen efter betalingslovens § 100.

Betalingsloven gør dermed endeligt op med hæftelsen og ansvarsfordelingen mellem betaleren og udbyderen, og der er ikke efterladt rum til, at et pengeinstitut kan tilpligtes at erstatte en kundes tab i tilfælde, hvor kunden selv har autoriseret transaktionen.

A autoriserede selv de omtvistede overførsler ved brug af sin egen netbank, og Nordea hæfter derfor hverken efter betalingslovens § 99 eller § 100.

As overførsler var autoriserede, jf. betalingslovens § 82, stk. 1, og Nordea hæfter derfor ikke efter betalingslovens § 99

Det følger af betalingslovens § 99, at betalerens udbyder af betalingstjenester hæfter i forhold til betaleren for tab som følge af uautoriserede betalingstransaktioner, medmindre andet følger af § 100.

Betalingslovens § 82 fastslår, at en betalingstransaktion kun er autoriseret, hvis betaleren har meddelt samtykke til at gennemføre

transaktionen (stk. 1), og at samtykke meddeles i den form, der er aftalt mellem betaleren og dennes udbyder (stk. 2). Det fremgår blandt andet af bemærkningerne til betalingslovens § 82, at der ved samtykke forstås godkendelse af en betaling fra bankkunden til dennes bankudbyder, eksempelvis ved betalerens brug af sin kode i netbank.

Spørgsmålet om, hvorvidt en betaling er autoriseret eller uautoriseret, afhænger alene af, om transaktionen bliver godkendt af kunden på den måde, som er aftalt mellem kunden og banken.

Det fremgår af Netbankaftalen, at overførsler skal ske ved anvendelse af NemID (nu: MitID). Det er i sagen ubestridt, at A selv foretog og godkendte samtlige transaktioner ved brug af sit NemID, ligesom hun bekræftede hver transaktion ved at svare "ja" til sms-bekræftelserne fra Nordea.

As betalinger var dermed autoriserede af hende selv, og Nordea hæfter allerede derfor ikke efter betalingslovens § 99.

Det var A selv, som anvendte sin netbank ved overførslerne, og Nordea hæfter derfor ikke efter betalingslovens § 100

Nordea hæfter ikke for As tab i medfør af betalingslovens § 100, idet bestemmelsen forudsætter, at andre uberettiget har anvendt betalingstjenesten.

Dette er ikke tilfældet i As sag.

Det fremgår af bemærkningerne til betalingslovens § 100, at:

"Forslaget til § 100 fastlægger den ansvarsfordeling, som skal gælde, hvis et betalingsinstrument bruges af en person, som ikke er berettiget til at bruge det."

Betalingslovens § 100 finder alene anvendelse, hvis betalingsinstrumentet bruges af en person, som ikke er berettiget hertil. Dette vil blandt andet være tilfældet ved svindelformen 'phishing', hvor svindlerne frannarrer personer fortrolige oplysninger, f.eks. kortoplysninger og passwords, hvorefter svindlerne kan bruge personens betalingsinstrument. Det er derimod ikke tilfældet ved 'safe account fraud', hvor svindlerne narrer personer til selv at bruge betalingsinstrumentet.

Dette understøttes også af Det finansielle ankenævns omfattende praksis på dette område. I de 131 afgørelser om bedrageriske opkald, som er oplistet i ekstrakten, vurderede ankenævnet i 104 af sagerne, at pengeinstitutterne ikke hæftede, idet betalingstransaktionerne var foretaget af kunderne selv. Af de resterende 27 sager blev 23 sager afvist, fordi en afgørelse forudsatte bevisførelse i form af parts- og vidneforklaringer eller vedrørte erhvervskonti, 3 sager vedrørte uautoriserede overførsler, og 1 sag vedrørte et forældet forhold. Det følger dermed også af fast ankenævnspraksis, at pengeinstitutter ikke hæfter efter betalingslovens § 100, når kunden selv har foretaget (autoriseret) betalingen.

I dette lys har Europa-Parlamentet og Rådet fremsat og førstebehandlet forslag til en forordning om betalings tjenester (COD(2023)0210), hvori der er udformet en ny artikel 59 om "*Svig i form af at udgive sig for en anden*". Det fremgår af artikel 59(1), at:

... [citeret ovenfor i afsnittet om retsgrundlaget]

Forslaget til forordningen indebærer i sin nuværende form dermed en væsentlig ændring af det gældende direktiv 2015/2366 og betalingsloven, som implementerer dette direktiv. Betalingsudbydere vil efter forslaget fremadrettet – under visse betingelser – således hæfte for tab, som kunden er blevet påført, fordi denne er blevet narret til at foretage betalinger af en tredjemand, som udgiver sig for at være ansat hos eksempelvis politiet. Forordningen er endnu ikke vedtaget og indebærer en væsentlig ændring af den gældende retstilstand. Behovet for ny lovgivning bekræfter i sig selv, at betalingsudbydere ikke efter gældende ret er ansvarlige for de omhandlede svindeltilfælde. Det foreslås med forordningen i øvrigt ikke, at hæftelsen indtræder med tilbagevirkende kraft.

As gennemgang af forarbejderne til betalingsloven, betalingskortloven og betalingsmiddeloven samt synspunktet om, at Det finansielle ankenævns retlige vurdering er forkert, kan ikke føre til en anden fortolkning af betalingslovens § 100.

As betalinger blev gennemført ved hendes egen brug af netbank, og Nordea hæfter derfor ikke efter betalingslovens § 100.

Nordea hæfter ikke i medfør af aftalelovens § 30 om tredjemands svig

Indledning

Nordea hæfter ikke for As tab i medfør af aftalelovens § 30 om svig. A har således ikke godtgjort, at Nordea indså eller burde have indset, at hendes viljeserklæringer til Nordea var fremkaldt ved svig fra tredjemand.

Nordeas it-systemer, som er dedikeret til overvågning af svindel, er avancerede og baseret på monitorering af adfærd, der kan indikere, at det ikke er kunden selv, der foretager overførslerne. Nordeas systemer går derudover videre end de regulatoriske krav for overførsler via netbank, idet Nordea har indført 'second channel confirmation'.

Hverken aktivering af 'second channel confirmation' eller Nordeas generelle viden om 'safe account fraud' indebærer ond tro om den konkrete svindel, og der er i øvrigt ikke retligt grundlag for As anbringende om systemisk ond tro.

Aktiveringen af 'second channel confirmation' indebærer ikke, at Nordea var i ond tro om svindlen af A

As synspunkt om, at Nordea opdagede svindlen i kraft af den 'second channel confirmation' (sms'er med anmodning om bekræftelse på overførslen ved at svare "ja"), der blev udløst i forbindelse med hendes overførsler, bestrides. Synspunktet beror på en misforståelse af den ekstra sikkerhedsforanstaltningsfunktion.

'Second channel confirmation' udløses ikke alene ved højrisiko-overførsler, men også ved overførsler af store beløb, som forklaret for byretten af Lucja Wägander, Strategic Project Leader i Fraud Management hos Nordea. Der kan være mange grunde til, at en kunde ændrer sit adfærdsmønster og ønsker at overføre et større beløb. 'Second channel confirmation' er derfor ikke en advarsel eller alarm om igangværende svindel, men en integreret del af de kontrolforanstaltninger, som Nordea har indført for at beskytte sine kunder.

A bekræftede ved hver enkelt 'second channel confirmation', at hun ønskede, at overførslerne skulle gennemføres, idet hun aktivt svarede "ja" til sms-bekræftelserne fra Nordea.

Sikkerhedsforanstaltningen medførte ikke, at Nordea indså eller burde have indset svindlen.

Nordeas generelle viden om 'safe account fraud' før august 2022 indebærer ikke, at Nordea var i ond tro om svindlen af A

Nordeas generelle viden om 'safe account fraud' giver ikke grundlag for at anse Nordea for at være i ond tro om den konkrete svindel af A.

'Safe account fraud' var en forholdsvis ny svindelmetode, da A blev svindlet, og sagstypen fik således også først sin egen indberetningskategori hos Finans Danmark i første kvartal af 2023.

Nordea har ikke bestridt, at banken på tidspunktet for As overførsler kendte til svindelmetoden. Nordea havde således blandt andet i maj 2022 en advarsel om telefonopkald fra svindlere på sin hjemmeside (...). Dette kendskab medfører imidlertid ikke, at Nordea generelt var i ond tro om svindeltypen, endsige at Nordea var i ond tro om den konkrete svindel, som A blev udsat for.

Nordea var ikke i "systemisk ond tro" om svindlen

Der er ikke retligt grundlag for As anbringende om "systemisk ond tro".

Vurderingen af ond tro er subjektiv i den forstand, at retten skal forholde sig til, hvad en fysisk person burde indse i den konkrete situation. Et system kan ikke i sig selv være i ond tro, og der må i stedet føres bevis for, at en eller flere medarbejdere i Nordea har været i ond tro om svindlen.

Det er ubestridt, at ingen medarbejdere hos Nordea har været i ond tro om svindlen, og det er allerede derfor udelukket, at Nordea kan anses for at have været i systemisk ond tro.

Under alle omstændigheder kan Nordea ikke anses for at have været i "systemisk ond tro", idet alle Nordeas systemer var i overensstemmelse med regulatoriske krav og branchenormer.

As henvisning til Sveriges Högsta Domstols afgørelse af 1. juli 2025 (sag T 607-24) kan ikke føre til et andet resultat. Dommen vedrørte en onlinespilletjenestes erstatningsansvar for markedsføring over for en spiller med diagnosticeret ludomani. Spilletjenesten anvendte teknologi til indsamling og behandling af data om individuelle kunders adfærd som grundlag for at sende automatiserede tilbud. Domstolen fastslog, at selskabet måtte anses for bekendt med de oplysninger, som teknologien gav adgang til, og at selskabet på baggrund af de indsamlede data burde have vidst, at brugeren havde alvorlige spilleproblemer.

Nordeas overvågningssystemer adskiller sig dermed væsentligt fra den online spilletjenestes systemer. Lucja Wägander, Strategic Project Leader i Fraud Management hos Nordea, forklarede for byretten, at Nordeas overvågningssystem består af regler, der ikke er *"baserede på den enkelte kundes betalingsmønstre, fordi kundernes historiske adfærd ikke altid fortsætter i fremtiden."* Reglerne er derfor i stedet *"baserede på information om forskellige typer af svindel, som de har fra data i systemet, og fra oplysninger om, hvad der sker i markedet."*

As viljeserklæringer er ikke ugyldige i medfør af aftalelovens §§ 36 og 38 c

As synspunkt om, at Netbankaftalen er ugyldig i medfør af aftalelovens §§ 36 og 38 c, fordi aftalen angiveligt har påført hende risikoen for et uventet og betydeligt tab, bestrides.

Netbankaftalen er hverken urimelig eller i strid med redelig handle-måde, jf. aftalelovens § 36, eller i strid med hæderlig forretningsskik, jf. aftalelovens § 38 c. Aftalen giver A adgang til netbanken, og flere af vilkårene for brug af netbank, herunder de for tvisten relevante, er udformet i overensstemmelse med betalingslovens bestemmelser.

A har i øvrigt ikke godtgjort, hvilken retsvirkning det skal have, hvis Netbankaftalen skal anses for ugyldig, herunder hvilken betydning det skal have for de overførsler, som hun har gennemført via sin netbank.

Nordea er ikke erstatningsansvarlig for As tab

Nordea er ikke erstatningsansvarlig for As tab, og hendes synspunkt om, at Nordea har pådraget sig et erstatningsansvar ved at indrette sin betalingstjeneste på en måde, som udsatte kunderne for en nærliggende risiko for tab, bestrides.

Nordea har overholdt sine kontraktuelle forpligtelser, regulatoriske krav, branchenormer og god skik. Der er derfor ikke grundlag for As synspunkt om, at Nordea har handlet ansvarspådragende i forbindelse med As tab.

Under alle omstændigheder er det ikke godtgjort, at As tab er en følge af Nordeas eventuelle undladelser, og en eventuel erstatning bør bortfalde eller nedsættes som følge af As egen skyld.

Nordea har ikke handlet ansvarspådragende

Indledning

Nordea har ikke handlet ansvarspådragende, idet Nordea løbende optimerer sine kontrolforanstaltninger for at beskytte sine kunder mod nye svindelmetoder, ligesom Nordea har rådgivet og advaret om svindel i overensstemmelse med god skik. Nordeas sikkerhedsforanstaltninger indebærer ikke en ansvarspådragende adfærd, og Nordeas systemer er ikke i strid med branchenormer.

Nordea optimerer løbende sine kontrolforanstaltninger for at beskytte sine kunder mod nye svindelmetoder

Nordea har løbende tilpasset og optimeret sine kontrolforanstaltninger i takt med udviklingen i svindelmetoderne.

Nordea havde i august 2022 (og har fortsat) it-systemer dedikeret til overvågning af svindel, som overvågede samtlige overførsler. Systemerne er opbygget med individuelle detektionsregler målrettet specifikke svindelmetoder. Lucja Wägander forklarede for byretten, at *"[r]eglerne er opbygget internt i Nordea og bliver dagligt optimeret"*. Nordeas overvågningssystemer kontrollerer alle overførsler, herunder om de ydre forhold indikerer, at det er kunden selv, der foretager overførslen, for eksempel om den foretages fra en kendt IP-adresse. Det er ubestridt, at alle ni transaktioner i nærværende sag blev foretaget fra den samme enhed og IP-adresse, som A normalt brugte ved netbanksoverførsler.

As antagelser om, hvordan Nordea kunne indrette sine systemer og muligheden for at overvåge transaktioner, indebærer reelt et objektivi ansvar for pengeinstitutterne i strid med lovgivers ønske om, at betalingsloven endeligt gør op med ansvarsfordelingen mellem kunde og pengeinstitutter i sager, hvor kunden selv har autoriseret overførslen.

Synspunktet om, at det var ansvarspådragende for Nordea at give sine kunder mulighed for at gennemføre straksoverførsler, er afkoblet fra de bredere samfundsmæssige hensyn til en smidig betalingsinfrastruktur. Straksoverførsler tilbydes af alle pengeinstitutter og blev indført på initiativ af Nationalbanken i 2014 med en beløbsgrænse på 500.000 kr. På daværende tidspunkt vægtede Nationalbanken hensynet til, at borgerne og virksomhederne hurtigt kunne gennemføre overførsler, højt, og det var først i november 2023, at det fra branchens side blev anbefalet at ændre denne beløbsgrænse.

Nordea ændrede tilsvarende sine beløbsgrænser for straksoverførsler. Den 12. april 2023 blev beløbsgrænsen således nedsat fra 500.000 kr. til 100.000 kr. for straksoverførsler, og den blev yderligere nedsat til 50.000 kr. den 19. december 2023.

As synspunkt om, at pengeinstitutter kan træffe simple forholdsregler mod svindel, kan heller ikke tiltrædes. Finans Danmark fandt det nødvendigt at nedsætte en Svindel Task Force i december 2023, som havde til formål at finde nye løsninger til at bekæmpe digital svindel. Bekæmpelse af svindel er en dynamisk opgave, da svindelmetoderne hele tiden ændrer sig. Svindel Task Forcen konkluderede også, at bekæmpelse af svindel er en fællesopgave, der ikke kan klares af en aktør alene.

Nordea har rådgivet og advaret i overensstemmelse med god skik

Nordea yder efter omstændighederne konkret rådgivning til sine kunder, når der udløses en alarm i Nordeas svindelovervågning.

Forud for august 2022 havde Nordea løbende advarsler på sin hjemmeside, netbank og sociale medier om forskellige former for svindel, hvor Nordea bad sine kunder udvise agtpågivenhed.

I april 2022 deltog Nordea i et interview på TV 2 Lorry om telefonsvindel, og i juni 2022 oprettede Nordea et opslag på sin Facebookside med advarsler om digital svindel, herunder med budskabet *"Lav aldrig en overførsel, fordi nogen forsøger at overtale dig til det over telefonen"*.

I maj 2022 havde Nordea følgende advarsel i en gul bjælke på forsiden af sin hjemmeside og loginsiden til netbank, hvor der blandt andet blev advaret om ikke at overføre penge til modtagere, som kunden ikke kendte:

"ADVARSEL OM TELEFON-OPKALD FRA SVINDLERE: Flere kunder modtager i øjeblikket opkald fra svindlere, som udgiver sig for at være fra fx digitaliseringsstyrelsen, politiet eller banken. Formålet er at franarre dig information som NemID eller MitID oplysninger, CPR-nummer eller kortoplysninger. Udlever ALDRIG disse informationer og overfør ikke penge til modtagere, du ikke kender. Vi håber, du vil hjælpe med at dele budskabet til dine nærmeste."

Det er ikke muligt at foretage konkret rådgivning om svindel, medmindre der udløses en alarm i et af Nordeas it-systemer, da det ellers ville kræve realtidsovervågning af alle transaktioner. Lucja Wägander, Strategic Project Leader i Fraud Management hos Nordea, forklarede for byretten, at der hvert sekund foretages mere end 100.000 transaktioner.

Der findes ingen regulatoriske krav om, at pengeinstitutter skal have realtidsovervågning eller blokeringsmekanismer med henblik på forebyggelse af svindel. Finans Danmark har i sit biinterventionsindlæg for byretten af 16. december 2024 fremhævet, at realtidsovervågning risikerer at medføre, at banktjenester *"bliver mere tidskrævende og mindre effektive og dermed dyrere og mindre tilgængelige for kunderne"*.

Der gælder endvidere ikke en pligt for pengeinstitutter til at yde rådgivning i forbindelse med overførsler via netbank, da disse udgør rene ekspeditioner. Det følger af vejledningen til bekendtgørelsen om god

skik for finansielle virksomheder, at der ikke er pligt til at yde rådgivning, hvis kunden alene efterspørger rene ekspeditioner, herunder pengeoverførsler. Overførsler i netbank er en standardiseret tjeneste, som kunden selv udfører, og Nordea er derfor ikke forpligtet til at rådgive om risikoen for svindel ved hver enkelt transaktion.

A anmodede ikke selv Nordea om rådgivning, og Nordea kan ikke pålægges en pligt til at foretage realtidsovervågning, da lovgivningen ikke indeholder krav herom.

Nordeas sikkerhedsforanstaltninger indebærer ikke ansvarspådragende adfærd

Det følger af betalingslovens § 128, at elektroniske betalingstransaktioner skal godkendes ved stærk kundeautentifikation (to-faktor-autentifikation). NemID (nu: MitID) udgør en sådan stærk kundeautentifikation.

Nordea har ved at kræve stærk kundeautentifikation dermed overholdt betalingslovens regler.

Nordeas sikkerhedsforanstaltning i form af en sms, som skal godkendes af bankkunden, før en betaling gennemføres ('second channel confirmation'), er ikke et lovkrav, men en ekstra sikkerhedsforanstaltning, som Nordea på eget initiativ har indført.

Det forhold, at Nordea i de pågældende sms'er i dag konkret advarer om svindel, er et udslag af den stigende svindel, der har fundet sted siden 2022. Forholdet støtter derfor ikke As synspunkt om, at Nordea skulle have handlet ansvarspådragende ved ikke at have de pågældende advarsler i 2022.

Nordeas systemer er ikke i strid med branchenormer

Det bestrides, at Nordeas it-systemer skulle være i strid med branchenormer eller på anden måde indrettet på ansvarspådragende vis. A har ikke ført bevis for den branchenorm, som Nordeas ansvar skal vurderes i forhold til, men alene søgt at støtte ret på en række synspunkter om, hvordan banksystemet ifølge hende burde være indrettet.

Byretten gav Nordea medhold i dette synspunkt og anførte herom: *"Eter bevisførelsen er der ikke fremkommet oplysninger om, at der i august 2022 fandtes en branchenorm for indretning af pengeinstitutters overvågning af svindel foretaget via netbank og bekæmpelse heraf".*

I mangel af andre beviser må den målestok, som Nordeas systemer skal bedømmes efter, være den standard, som Højesteret lagde til grund i søgsmålet mod Domstolsstyrelsen vedrørende det digitale tinglysningssystem, jf. U.2020.2851H, hvorefter ansvar forudsætter, at der i forbindelse med indretningen af it-systemer skal påvises væsentlige og klare fejl eller forsømmelser.

Det svarer til Norges Høyesteretts dom af 31. maj 2024 (sagsnr. 23-101291SIV-HRET), præmis 82, hvor det anføres, at bankerne som udgangspunkt selv må vurdere, hvordan de vil indrette deres systemer, når der ikke foreligger branchepraksis om sikkerhedsniveauet.

Antallet af sager, som Nordea er involveret i ved Det finansielle ankenævn, er ikke dokumentation for, at andre banker har bedre kontrolforanstaltninger til imødegåelse af svindel. Nordea er ikke bekendt med årsagen til fordelingen, men det kan skyldes mange forskellige forhold, for eksempel at Nordea fastholder, at banken ikke er erstatningsansvarlig for den udøvede svindel, eller at Nordea er bedre til at vejlede sine kunder om klagemuligheder. Statistikken siger i øvrigt alene noget om fordelingen af klagesager – ikke om årsagerne bag fordelingen, og den kan derfor ikke uden videre anvendes som grundlag for en kvalitativ sammenligning af bankernes interne procedurer eller kontrolforanstaltninger.

Selv hvis det lægges til grund, at andre pengeinstitutter havde truffet bedre kontrolforanstaltninger end Nordea til imødegåelse af svindel på tidspunktet for As betalinger, dokumenterer dette ikke, at Nordea ved ikke at træffe tilsvarende kontrolforanstaltninger har handlet ansvars-pådragende.

As tab er ikke en følge af Nordeas eventuelle undladelser

A har ikke dokumenteret, at hendes tab er en følge af Nordeas eventuelle undladelser. Herunder har hun ikke godtgjort, at hun ikke ville have gennemført transaktionerne, selv hvis Nordeas systemer havde opdaget et usædvanligt transaktionsmønster, eller hvis hun var blevet rådgivet konkret om risikoen for svindel. A har således også selv forklaret, at hun var opmærksom på risikoen for, at der var tale om svindel, men at hun alligevel overførte beløbene.

A har heller ikke godtgjort, at hendes tab ville være begrænset til 100.000 kr., hvis beløbsgrænsen for straksoverførsler havde været 100.000 kr. i stedet for 500.000 kr. på tidspunktet, hvor hun blev svindlet.

En eventuel erstatning bør bortfalde eller nedsættes som følge af den af A udviste egen skyld

Hvis landsretten finder, at Nordea er erstatningsansvarlig for As tab, gør Nordea gældende, at erstatningen bør bortfalde, subsidiært nedsættes, som følge af den af A udviste egen skyld.

Det var A selv, der foretog samtlige ni overførsler over to dage. Det fremgår af hendes egen gengivelse af hændelsesforløbet, at hun var bevidst om, at der var en risiko for, at hun blev udsat for svindel. Hun indvilligede dermed i risikoen, da hun besluttede at foretage transaktionerne.”

Nordea, som har angivet at være delvist momsregistreret, har oplyst, at banken ikke kan afløfte moms for så vidt angår advokatudgiften i denne sag

Landsrettens begrundelse og resultat

Sagen angår som for byretten spørgsmålet om, hvorvidt Nordea helt eller delvist skal friholde A for det tab på 398.957,62 kr., hun har lidt ved at ukendte gerningsmænd under telefonopkald til hende bedragerisk har fået hende til at foretage ni bankoverførsler af et samlet beløb på 416.665 kr. til af gerningsmændene anviste konti, hvoraf alene et beløb på 17.707,38 kr. er tilbageført til A.

A har gentaget sine anbringender for byretten, idet hun dog har frafaldet anbringenderne om ugyldighed efter aftalelovens § 28 og § 29, om at Nordea hæfter i medfør af vilkårene i parternes netbanksaftale, og om at Nordea havde en burde-viden efter reglerne i hvidvaskloven. A har herudover fremsat et nyt anbringende om, at det er ansvarspådragende, at Nordea ikke straks sikrede tilbageførsel ved As henvendelse ved fysisk fremmøde om formiddagen den 23. august 2022 straks efter misbruget den foregående aften.

Autoriseret betalingstransaktion (samtykke) efter betalingsloven

Af forarbejderne til § 82, stk. 1, i den gældende betalingslov fra 2017 om, hvornår betalingstransaktioner skal anses for autoriserede, fremgår, at bestemmelsen gennemfører artikel 64 i andet betalingstjenestedirektiv. Den tidligere gældende bestemmelse om, hvornår betalingstransaktioner anses for autoriserede i § 57, stk. 1, i betalingstjenesteloven fra 2009, gennemførte ifølge forarbejderne hertil på samme måde artikel 54 i første betalingstjenestedirektiv, som svarer til artikel 64 i andet betalingstjenestedirektiv. Bestemmelsen i § 82, stk. 1, skal herefter og efter forarbejdernes indhold i øvrigt forstås i overensstemmelse med artikel 64 i andet betalingstjenestedirektiv.

I forslaget til Europa-Parlamentet og Rådets forordning om betalingstjenester i det indre marked og om ændring af forordning (EU) nr. 1093/2010, COM(2023) 366, er det ved bestemmelsen i artikel 59, jf. også præambelbetragtning 79 og 80, foreslået at give forbrugere, der ved svigagtig manipulation vildledes til at godkende betalingstransaktioner, en bedre beskyttelse end efter de nugældende regler. Efter den foreslåede bestemmelse skal udbyderen af betalingstjenester således som udgangspunkt tilbagebetale forbrugeren det fulde beløb for den svigagtige autoriserede betalingstransaktion i tilfælde, hvor gerningsmanden har foregivet at være ansat hos forbrugerens udbyder af betalingstjenester ved ulovlig brug af den pågældende betalingstjenesteudbyders navn eller e-mail-adresse eller telefonnummer, og denne manipulation har givet anledning til efterfølgende svigagtige autoriserede betalingstransaktioner.

Landsretten finder, at det følger af ordlyden af betalingsloven og forarbejderne hertil sammenholdt med den tilgrundliggende direktivbestemmelse og det

ovenstående forslag, at betalingslovens § 82, stk. 1, må forstås således, at der foreligger samtykke og dermed en autoriseret betalingstransaktion i bestemmelsens forstand, hvis betaleren selv foretager og godkender overførslen i den med udbyderen aftalte form. Det er i den forbindelse uden betydning, om betaleren under bedrageriske telefonopkald er blevet narret og presset til at foretage overførslen og har været i en ved det bedrageriske telefonopkald fremkaldt vildfarelse om formålet med overførslen.

Herefter og af de grunde, som byretten har anført, må A anses for at have givet samtykke efter betalingslovens § 82, stk. 1, til de ni overførsler. Nordea hæfter derfor ikke for hendes tab i medfør af betalingslovens § 100, stk. 1, 1. pkt.

Aftalelovens § 36 og § 38 c

Af de grunde, byretten har anført, tiltræder landsretten, at den mellem A og Nordea indgåede netbankaftale af 16. december 2002 ikke kan anses for at være urimelig eller i strid med redelig handlemåde. Det kan heller ikke anses for stridende mod hæderlig forretningsskik og bevirke en betydelig skævhed i parternes rettigheder og forpligtelser til skade for forbrugeren, at Nordea gør de aftalte vilkår gældende. Der er følgelig ikke grundlag for delvist at ændre eller tilsidesætte aftalen i medfør af aftalelovens § 36 eller § 38 c.

Aftalelovens § 30, stk. 1, og erstatningsansvar

Det er ubestridt, at A har været udsat for svig som nævnt i aftalelovens § 30, stk. 1. Spørgsmålet er, om Nordea indså eller burde have indset, at hendes viljeserklæringer i form af samtykke til de ni overførsler var afgivet som følge af svig fra tredjemands side, eller om Nordea er erstatningsansvarlig for As tab.

Som anført af byretten er de ni overførsler sket fra samme enhed og IP-adresse, som A normalt brugte ved gennemførelse af transaktioner på netbank. Nordeas netbanksystem er indrettet således, at As digitale godkendelse af hver af de ni overførsler udløste en sms-anmodning til As mobiltelefon om at oplyse, om hun ønskede at gennemføre transaktionen, hvilket hun i alle ni tilfælde besvarede bekræftende.

Efter det af Nordea oplyste om, hvornår de beløb, som A overførte til modtagerkonti i Nordea, blev hævet, lægger landsretten til grund, at i hvert fald hovedparten af de overførte beløb blev hævet fra de pågældende konti kort efter As overførsler, og dermed inden A om morgenen den 23. august 2022 henvendte sig til Nordea.

Det må efter den bevisførelse, der har været for landsretten, herudover lægges til grund, at svig i form af bedrageriske telefonopkald var et kendt fænomen i banksektoren i august 2022, og at fænomenet var velbekendt for Nordea. Nordea havde således i august 2022 været eller var indklaget i Det Finansielle

Ankenævn i ni klagesager om hæftelse for svig ved bedrageriske telefonopkald, begået før A blev udsat for sådant svig, og Nordea havde den 28. september 2021 advaret mod svig af denne type på en underside på bankens hjemmeside. Strategic Project Leader i Nordea, Lucja Wägander har forklaret, at Nordea foretager adfærdsmonitoring i realtid i netbank og mobilbank, som hvis der udløses en alarm sendes til et team, som håndterer advarslen eller automatisk kan spærre kundens forbindelse. Det pågældende automatiske monitoreringssystem er ifølge det forklarede etableret med henblik på at opfylde kravene i andet betalingstjenestedirektiv, hvormed nærmere må menes direktivets artikel 95-98, og de i medfør af artikel 98 udstedte Regulatory Technical Standards i Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366. Efter de i sagen foreliggende oplysninger lægger landsretten til grund, at systemet ikke på det tidspunkt, hvor A var udsat for de bedrageriske telefonopkald, var indrettet på en måde, som medførte, at det advarede om overførsler, som dem A foretog, endsige at sådanne overførsler blev stoppet. Der er heller ikke oplysninger om, at systemet i dag indeholder sådanne funktioner.

Udbydere af betalingstjenester som Nordea er ikke lovgivningsmæssigt forpligtet til at foretage overvågning af kunders betalingsmønstre med henblik på at opdage og gribe ind over for bedrageriske telefonopkald. Det følger som allerede nævnt af betalingsloven og det til grund herfor liggende betalingstjenestedirektiv, at udbydere af betalingstjenester ikke hæfter for tab ved sådan svindel.

Der er heller ikke for landsretten oplysninger, som understøtter, at der på daværende tidspunkt var branchekutymer om systemmæssig overvågning og andre tiltag, herunder nedsættelse af beløbsgrænser for straksoverførsler eller advarsler til kunder, der havde til formål af forebygge og bekæmpe bedrageriske telefonopkald.

På den nævnte baggrund kan det ikke antages, at Nordea indså eller burde have indset, at As autorisation af de ni overførsler var fremkaldt ved svig fra tredjemands side, jf. aftalelovens § 30, stk. 1.

Efter det oplyste om indretningen af Nordeas betalingssystem i netbank og de af Nordea på daværende tidspunkt gennemførte sikkerhedsforanstaltninger sammenholdt med det ovenfor anførte tiltræder landsretten endvidere, at der ikke er grundlag for at anse Nordea for erstatningsansvarlig for As tab. Der er herunder ikke grundlag for et ansvar som følge af for sen iværksættelse af forsøg på tilbageførsel.

Resultat og sagsomkostninger

Landsretten stadfæster dermed byrettens frifindende dom.

Efter sagens udfald skal As retshjælpsforsikring, i det omfang den dækker, subsidiært statskassen, i sagsomkostninger for landsretten betale 90.000 kr. til Nordea til dækning af udgifter til advokatbistand inkl. moms. Ud over sagens værdi er der ved fastsættelsen af beløbet taget hensyn til sagens omfang, forløb og principielle betydning.

Biintervenienten, Finans Danmark, bærer egne omkostninger.

THI KENDES FOR RET:

Byrettens dom stadfæstes.

I sagsomkostninger for landsretten skal As retshjælpsforsikring i Alka Forsikring (skadenr. 3769425-T01MEMI), i det omfang den dækker, subsidiært statskassen, inden 14 dage betale 90.000 kr. til Nordea Danmark, Filial af Nordea Bank Abp, Finland.

Beløbet forrentes efter rentelovens § 8 a.

Biintervenienten, Finans Danmark, bærer egne omkostninger.