Indsigelse mod korttransaktioner efter telefoniske henvendelser. Videregivelse af kortoplysninger og sms-koder samt oplysninger, der gav adgang til klagerens computer via Teamviewer.

Sagsnummer:	280/2019
Dato:	07-11-2019
Ankenævn:	Vibeke Rønne, Inge Kramer, Peter Stig Hansen, Morten Bruun Pedersen, Poul Erik Jensen
Klageemne:	Betalingstjenester - groft uforsvarlig adfærd Betalingstjenester - ikke groft uforsvarlig adfærd Betalingstjenester - ubegrænset hæftelse
Ledetekst:	Indsigelse mod korttransaktioner efter telefoniske henvendelser. Videregivelse af kortoplysninger og sms-koder samt oplysninger, der gav adgang til klagerens computer via Teamviewer.
Indklagede:	BankNordik
Øvrige oplysninger:	OF
Senere dom:	
	Pengeinstitutter

Delvis medhold.

Indledning

Sagen vedrører indsigelse mod korttransaktioner i forbindelse med telefoniske henvendelser.

Sagens omstændigheder

Klageren var kunde i BankNordik, hvor han havde en konto med et tilknyttet Visa/dankort.

Den 18. februar 2019 kl. 12.51 blev klageren ringet op af en person, P1, som udgav sig for at være fra Microsoft. P1 oplyste, at klagerens computer havde en sikkerhedsbrist, at den havde været udsat for forsøg på hacking, og at P1 kunne rette fejlene og sørge for, at klageren fik købesummen for computeren tilbage. P1 fik adgang til klagerens computer via programmet Teamviewer. Klageren har oplyst, at han videregav sine kortoplysninger, personnummer og et foto af sit kørekort til P1 til brug for at få tilbageført købesummen for computeren.

Samme dag kl. 17 blev klageren ringet op af endnu en person, P2, som udgav sig for at være fra Microsoft og som oplyste, at hun ville overføre købesummen for computeren til klagerens konto i kryptovaluta. P2 tilbød klageren software til 100 USD til beskyttelse af hans computer, hvilket klageren sagde ja til. Klageren har oplyst, at P2 ringede til ham dagen efter, og at han oplyste de engangskoder, som han fik tilsendt pr. sms til sin telefon, til P2.

Banken har fremlagt en udskrift fra Nets vedrørende afsendelse af tre sms-beskeder med 3d-secure koder til klagerens telefonnummer den 18. februar 2019 kl. 13.10.51, 17.27.32 og 19.02.32. Banken har fremlagt eksempler på sms-beskeder sendt fra Nets med engangskoder til køb på internettet. Sms-beskederne indeholdt følgende:

”Din engangskode er:

[…] til dit køb på [beløb] DKK hos [forretning eller hjemmeside].

Er du ikke i gang med onlinehandel, spær straks kortnr. […]!”

Banken har fremlagt en udskrift fra sit IT-system vedrørende 3D-secure godkendelse af tre transaktioner med klagerens kort den 18. februar 2019 på i alt 12.796,86 DKK (5.035,00 DKK kl. 13.19.38, 762,20 DKK kl. 17.28.38 og 928,71 EUR kl. 19.03.09) til Western Union og to andre betalingsmodtagere, der var registreret som ”quasi cash” virksomheder.

Den 20. februar 2019 blev der via klagerens kort gennemført betalinger på 5.035 DKK, 6.999,66 DKK (928,71 EUR), 762,20 DKK og 382,27 DKK (50,72 EUR) til Western Union og de to andre betalingsmodtagere.

Klageren har oplyst, at han dagen efter telefonsamtalerne med P2 tjekkede sine sms’er og fik mistanke om, at der var noget galt, hvorefter han spærrede sit kort og anmeldte sagen til politiet. Klageren indgav endvidere en indsigelse til banken, der afviste indsigelsen.

Parternes påstande

Den 22. juli 2019 har klageren indbragt sagen for Ankenævnet med påstand om, at BankNordik skal tilbageføre 12.796,86 DKK til ham.

BankNordik har nedlagt påstand om principalt frifindelse, subsidiært afvisning og mere subsidiært, at klageren skal hæfte med 8.000 DKK.

Parternes argumenter

Klageren har anført, at hans kort er blevet misbrugt.

P1 overbeviste ham om, at hans computer havde en sikkerhedsbrist, og at der var forsøg på indbrud i computeren. P1 oplyste sit medarbejder nummer og nummeret på hans computer. P1 fik adgang til Teamviewer og viste, at der var en række fejl på computeren. P1 skrev en e-mail til Microsoft, hvori P1 beskrev problemerne med computeren, og meddelte, at han forlangte pengene tilbage. P1 fik hans kreditkortoplysninger, så beløbet ville kunne blive overført til kortet. P1 skulle også bruge hans personnummer og hans id.

P2 præsenterede sig også som "Microsoft" medarbejder og oplyste et langt licensnummer. P2 sagde, at pengene for computeren ville blive overført til hans bankkonto med kryptovaluta, og at hun derfor ville oprette ham hos nogle ”exchanges”. P2 tilbød noget software til 100 dollar, som kunne beskytte hans computer, hvilket han takkede ja til. P2 ringede igen næste dag og sagde, at han skulle oplyse de koder, som blev sendt til hans telefon via sms. Der kom en række koder pr. sms, som han oplyste til P2. Han var i gang med andre gøremål imens, så han bemærkede ikke, at der på et tidspunkt kom sms, som omhandlede overførsel af penge, men oplyste bare koderne. Først næste dag, da han kiggede sine sms’er igennem, fik han mistanke om, at der noget var galt og spærrede kortet.

Han har efterfølgende via glemt password funktionen haft held til at finde ud af, at P1/P2 oprettede en e-mail adresse i hans navn. Han fandt også ud af, hvilke dispositioner P1/P2 foretog. Der blev foretaget en transaktion fra Western Union til en person i Columbia, som eventuelt kunne være P2. Han har kontaktet Western Union med disse oplysninger og har fået et sagsnummer. Han har fået lukket de fleste af de konti, han blev oprettet med. Han har meldt episoden til politiet, som behandler sagen, men han har endnu intet hørt fra politiet.

Han var oppe imod nogle meget overbevisende kriminelle, som gjorde alt for at distrahere ham med mange koder på sms fra de ”exchanges” og e-mail konti, som de oprettede ham i, så han først for sent lagde mærke til, at to sms’er omhandlede pengeoverførsel.

Efterfølgende blev han klar over, at mange danskere er blevet bedraget og overtalt til at give følsomme oplysninger til "Microsoft" svindlere. Forbrugerbeskyttelse i en sådan situation burde være en selvfølge i et retssamfund. BankNordik har ikke løftet bevisbyrden for, at han ikke er blevet bedraget. Han anmodede banken om erstatning, da han var sikker på, at banken var forsikret mod den slags svindel, og at banken var forpligtet til at betale erstatning ifølge lovgivningen om forbrugerbeskyttelse. Bankens afvisning var begrundet med, at han ikke havde en kvittering fra svindlerne. Denne begrundelse er ikke tilstrækkelig til at afvise hans anmodning.

BankNordik har til støtte for frifindelsespåstanden anført, at klageren gav samtykke til at gennemføre transaktionerne. Der var ikke tale om uautoriserede betalinger, og derfor har klageren ikke ret til tilbagebetaling. Alternativt må der ske frifindelse af banken, jf. betalingslovens § 100, stk. 5, idet klageren med forsæt oplyste den personlige sikkerhedsforanstaltning til den, der foretog den uberettigede anvendelse under omstændigheder, hvor klageren indså eller burde have indset, at der var risiko for misbrug.

Klageren gav uden nærmere undersøgelser P1/P2 adgang til sin computer via Teamviewer og udleverede sine kreditkortoplysninger, personnummer og kopi af sit kørekort. Klageren oplyste endvidere de sikkerhedskoder, som han modtog via sms-beskeder på trods af, at det i sms-beskederne udtrykkeligt fremgik, at klageren for hver kode godkendte, at et bestemt beløb blev trukket på hans kort. I hver enkelt sms-besked fremgik beløb og beløbsmodtager udtrykkeligt, ligesom sms-beskederne indeholdt en advarsel om, at man, hvis man ikke var i gang med at foretage en online handel, straks skulle spærre kortet. Klageren oplyste i sin klage, at han er klar over at: ”Utrolig mange danskere er blevet bedraget og overtalt til at give følsomme oplysninger til »Microsoft« svindlere…”. På trods heraf udleverede klageren alle oplysninger, som ”Microsoft” bad om. Bankens afvisning af indsigelsen var ikke begrundet med, at klageren ”ikke havde en kvittering fra svindlerne”.

BankNordik har til støtte for afvisningspåstanden anført, at banken har dokumenteret, at transaktionerne er korrekt registreret og bogført, og at de ikke har været ramt af tekniske svigt eller andre fejl, samt at den til kortet hørende personlige sikkerhedsforanstaltning blev anvendt i forbindelse med betalingstransaktionerne. Banken har dokumenteret, at sms’erne med den personlige sikkerhedsforanstaltning blev sendt til klagerens telefon. Banken har hermed løftet bevisbyrden jf. betalingslovens § 98, stk. 1, og det må herefter være op til klageren at bevise, at det ikke var ham, der godkendte transaktionerne. Dette forudsætter en yderligere bevisførelse i form af parts- og vidneafhøringer, der ikke kan ske for Ankenævnet, men som må finde sted ved domstolene. Ankenævnet må derfor afvise at behandle klagen.

BankNordik har til støtte for den mere subsidiære påstand anført, at klageren under alle omstændigheder må hæfte med 8.000 DKK, jf. betalingslovens § 100, stk. 4, nr. 3.

Ankenævnets bemærkninger

Den 18. februar 2019 blev der autoriseret tre betalingstransaktioner på i alt 12.796,86 DKK, med klagerens Visa/Dankort, der er udstedt af BankNordik, til Western Union og to andre betalingsmodtagere.

Baggrunden for transaktionerne var, at klageren den samme dag kl. 12.51 og kl. 17 var blevet kontaktet telefonisk af to personer, P1 og P2, der udgav sig for at være fra Microsoft, og som oplyste, at der var en sikkerhedsbrist ved klagerens computer, som de tilbød at rette. P1/P2 tilbød at sørge for, at klageren fik købesummen for computeren tilbage og tilbød endvidere, at klageren kunne købe software til 100 USD til beskyttelse af sin computer. Klageren gav herefter P1/P2 adgang til sin

computer via Teamviewer og udleverede sine kortoplysninger, personnummer og kopi af sit kørekort. Klageren oplyste endvidere de sikkerhedskoder, som han modtog via sms-beskeder, og som indeholdt oplysning om beløb og beløbsmodtager til P1/P2.

Ankenævnet finder det godtgjort, at transaktionerne skyldes tredjemands misbrug af klagerens Visa/dankort, og at misbruget også omfattede brugen af sms-koderne.

Det lægges endvidere til grund, at transaktionerne er korrekt registreret og bogført og ikke er ramt af tekniske svigt eller andre fejl, jf. betalingslovens § 98, stk. 1. Efter bestemmelsens stk. 2 er registrering af brug af et betalingsinstrument ikke i sig selv bevis for, at betaleren har godkendt transaktionen, at betaleren har handlet svigagtigt, eller at betaleren har undladt at opfylde sine forpligtelser, jf. betalingslovens § 93.

Ankenævnet finder, at sms-koderne var personlige sikkerhedsforanstaltninger til kortet, jf. betalingsloven § 7, nr. 31. Ved transaktionerne blev der anvendt stærk kundeautentifikation, jf. betalingsloven § 7, nr. 30.

Efter betalingslovens § 100, stk. 5, hæfter betaleren uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, og betalerens udbyder godtgør, at betaleren med forsæt har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede an-vendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug. Ankenævnet finder ikke, at banken har godtgjort, at betingelserne for, at klageren hæfter uden beløbsbegrænsning efter betalingslovens § 100, stk. 5 er opfyldt.

Efter betalingslovens § 100, stk. 4, nr. 2 og 3 hæfter betaleren med op til 8.000 DKK af tabet som følge af andres uberettigede anvendelse, hvis betalerens udbyder godt-gør, at betaleren med forsæt har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 5, eller at betaleren ved groft uforsvarlig adfærd har muliggjort den uberettigede anvendelse.

De til klageren sendte sms'er indeholdt oplysning om beløb og beløbsmodtager. Ankenævnet finder, at klageren ved at videregive engangskoderne ved groft uforsvarlig adfærd har muliggjort transaktionerne, og at klageren som følge heraf hæfter med op til 8.000 DKK. Ankenævnet har herved blandt andet lagt vægt på indholdet af "Microsofts" medarbejders "tilbud" til klageren, herunder om at købe computeren tilbage, og at købesummen ville blive overført i kryptovaluta.

BankNordik skal derfor tilbageføre differencen på 4.796,86 DKK til klagerens konto med valør fra datoen for debitering af transaktionerne.

Ankenævnets afgørelse

BankNordik skal inden 30 dage tilbageføre 4.796,86 DKK til klagerens konto som ovenfor anført.

Klageren får klagegebyret tilbage.