Indsigelse mod at hæfte for misbrug af betalingskort i forbindelse med phishing. Spørgsmål om, hvorledes der var sket anvendelse af engangskode sendt via SMS.

Sagsnummer:	165/2020
Dato:	30-10-2020
Ankenævn:	Bo Østergaard, Jesper Claus Christensen, Karin Duerlund, Ida Marie Moesby, Lisbeth Baastrup Burgaard.
Klageemne:	Betalingstjenester - ikke-vedkendte hævninger Betalingstjenester - ubegrænset hæftelse
Ledetekst:	Indsigelse mod at hæfte for misbrug af betalingskort i forbindelse med phishing. Spørgsmål om, hvorledes der var sket anvendelse af engangskode sendt via SMS.
Indklagede:	Bank Norwegian
Øvrige oplysninger:	OF IF
Senere dom:	
	Pengeinstitutter

Klager medhold.

Indledning

Sagen vedrører indsigelse mod at hæfte for misbrug af betalingskort i forbindelse med phishing. Spørgsmål om, hvorledes der var sket anvendelse af en engangskode sendt via SMS.

Sagens omstændigheder

Klageren havde et kreditkort, der var udstedt af Bank Norwegian. Til kortet var der knyttet en kredit på 40.000 kr.

Klageren har oplyst, at hun den 20. januar 2020 modtog en falsk mail med et fødselsdagstilbud, der fremstod som om, at den kom fra flyselskabet, F, som hun tidligere havde benyttet. Ifølge mailen kunne hun få en billig flybillet ved at indbetale 80 kr. Hun fulgte et link i mailen for at betale 80 kr. Hun indtastede sine kortoplysninger og fik efterfølgende sendt en engangskode via SMS til sit telefonnummer. Da det fremgik af SMS'en, at der ville blive trukket ca. 8.500 DKK, indtastede hun ikke engangskoden.

Banken har fremlagt en transaktionsliste indhentet via bankens leverandør, Evry, hvoraf fremgik, at der den 20. januar 2020 kl. 19:30:52 blev autoriseret en transaktion på 1.108 EUR vedrørende et køb hos en udenlandsk internetforretning, G, med klagerens kreditkort.

Banken har oplyst, at ifølge oplysningerne fra bankens leverandør, blev købet gennemført ved indtastning en engangskode, som den 20. januar kl. 19:29:54 var blevet sendt og leveret til klagerens telefonnummer via sikkerhedsløsningen 3D Secure/Verified by Visa. SMS-teksten var følgende:

"Engangskode [kode]. Til brug for køb på 1.108,00 EUR hos [H]. Kon- troller at beløb og brugersted er

korrekt."

Klageren gjorde efterfølgende over for banken indsigelse mod betalingen på 1.108 EUR, der den 21. januar 2020 blev trukket på hendes konto med 8.425,49 DKK. Hun anførte, at der var tale om en falsk mail fra F med tilbud, der lokkede med billig rejse.

I en mail af 22. februar 2020 til banken, hvori klageren redegjorde for, hvorledes hun havde forholdt sig med engangskoden sendt til hendes telefonnummer, anførte klageren følgende:

"Sms en er ikke blevet anvendt af mig. Jeg skulle betale 80,00 kr. på mit norwegian kort til jer.

Da sms kom frem var den rød og nogen havde hævet 1.100 euro på min konto og så stoppede jeg med det samme og fik mit kort spærret hos jer og ved Net[s] i DK.

Så var jeg klar over, at jeg var blevet hacket."

I en mail af 28. februar 2020 til klageren anførte banken følgende:

"**Om din indsigelse om ukendt transaktion**

Tak for dit svar. Vi har nu færdigbehandlet din indsigelse.

Banken kommer ikke til at dække dit tab, men vi holder dig ansvarlig for det bestridte beløb.

Verified by VISA

Den indklagede transaktion er foretaget med en sikker betalingsløsning over internettet (verified by VISA). Det vil sige, at der er benyttet dine kortoplysninger, kortets udløbsdato, kontrolkoden og den SMS-kode, der er sendt til dit telefonnummer den 20. januar 2020, klokken 19:29:54.

Sagens oplysninger

Du har oplyst, at du har modtaget denne besked på din mobiltelefon. Du oplyser også, at du ikke har benyttet engangskoden i SMS'en.

Du har også oplyst, at du ikke har mistet dit Norwegian-kort eller at det har været andre i hænde. Du har også oplyst, at der ikke er andre, der har tilgang til din mobiltelefon.

Du har videre oplyst, at du ikke selv har foretaget transaktionen hos [G]. Du har også oplyst, at du har modtaget flere phishing-mails.

Bankens vurdering

Uanset din redegørelse, så er de nødvendige oplysninger til at foretage den ovennævnte sikre transaktion på internettet blevet videregivet til uvedkommende. Herunder er koden i SMS'en blevet videregivet. Hvis ikke koden fra SMS'en var videregivet, så var det ikke muligt at gennemføre den bestridte transaktion.

Ved et internetkøb med en sikker betalingsløsning har salgsstedet erhvervet ret til betalingen. Bank Norwegian har således ikke mulighed for at sende dit krav videre til VISA for refundering fra salgsstedet.

Vi vurderer, at du har været udsat for phishing eller en lignende handling. Denne type svindel har stor opmærksomhed i medierne. Der er også ofte advarsler mod at trykke på links i mails og mod at udlevere sine kort- og sikkerhedsoplysninger.

Det fremgik af den fremsendte SMS hvilket køb, herunder beløb og brugersted, som den skulle benyttes til at godkende.

Det er derfor vores opfattelse, at du selv har forårsaget tabet ved en forsætlig handling.

Vi mener, at du ved modtagelsen af SMS'en burde have indset, at der var risiko for misbrug af dit kort.

Du holdes derfor ansvarlig for hele det bestridte beløb, jf. betalingslovens § 100, stk. 5.

…"

Klageren gjorde efterfølgende indsigelse mod bankens afvisning af hendes indsigelse, men banken fastholdt afvisningen.

Parternes påstande

Den 8. maj 2020 har klageren indbragt sagen for Ankenævnet med påstand om, at Bank Norwegian skal tilbageføre beløbet på 8.425,49 DKK.

Bank Norwegian har nedlagt påstand om frifindelse.

Parternes argumenter

Klageren har anført, at hun er blevet hacket og ikke kan vedkende sig den omtvistede transaktion.

Hun kender ikke noget til G, har ikke foretaget et køb hos G og har ikke indtastet den engangskode, som hun modtog i en SMS. Da hun i SMS'en så, at det drejede sig om et køb på ca. 8.500 DKK, stoppede hun omgående, og hun anvendte ikke engangskoden.

Banken har kun dokumenteret, at den har fremsendt engangskoden til hendes telefonnummer, men har ikke dokumenteret, at hun har indtastet engangskoden.

Hun er ikke i stand til at fremlægge en plausibel forklaring på, hvorfor transaktionen kunne gennemføres udover, at bankens sikkerhedssystem må have en brist.

Hun har i øvrigt ikke modtaget nogen ydelse fra G i forbindelse med transaktionen, og da transaktionen fremtræder som et køb på nettet, hvor hun ikke har modtaget nogen ydelse, bør hun ligeledes af den grund kunne få beløbet tilbageført.

Bank Norwegian har anført, at den omtvistede transaktion er blevet autoriseret af klageren selv. Det er ikke godtgjort, at der er tale om en uautoriseret transaktion. Kortnummer, udløbsdato og det trecifrede sikkerhedsnummer fra kortets bagside er oplyst. Transaktionen er autoriseret med en engangskode, som udelukkende er fremsendt til klageren på SMS. Klageren har bekræftet at have modtaget denne SMS. Hun bestrider at have videregivet engangskoden.

Beløb, valuta og salgssted fremgår tydeligt af SMS-teksten.

Klageren har også oplyst, at der ikke er andre, der har haft adgang til hendes telefon.

Uanset om Ankenævnet måtte komme frem til, at der er tale om en uautoriseret transaktion, mener banken subsidiært, at klageren skal hæfte for det fulde beløb, idet klageren selv har videregivet sine kortoplysninger og formentlig også engangskoden fra SMS, uanset at det af teksten i SMS'en klart fremgår, at koden godkender den pågældende betaling.

Det fremgår også, at transaktionen er i en anden valuta, end klageren mente, hun skulle foretage en transaktion i. Derfor mener banken, at klageren har været forsætlig i sin handling.

Hvis Ankenævnet ikke måtte komme frem til, at klageren har været forsætlig, så mener banken mere subsidiært, at klageren skal hæfte med en egenandel på 8.000 kr., da det var groft uagtsomt, at klageren videregav engangskoden, som blev fremsendt på SMS.

Ankenævnets bemærkninger

Den 20. januar 2020 blev der gennemført en betaling på 1.108 EUR svarende til 8.425,49 DKK med klagerens kreditkort udstedt af Bank Norwegian.

Ankenævnet lægger til grund, at transaktionen skete med 3D Secure, det vil sige på grundlag af en SMS-engangskode, som blev sendt til klagerens telefonnummer, samt på grundlag af kortoplysninger

bestående af kortnummer, udløbsdato samt det trecif- rede sikkerhedsnummer på bagsiden af kortet. Ankenævnet lægger endvidere til grund, at transaktionen er korrekt registreret og bogført og ikke ramt af tekniske svigt eller andre fejl, jf. lov om betalinger § 98. 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. lov om betalinger § 93.

Klageren har oplyst, at hun den 20. januar 2020 modtog en mail med et fødselsdagstilbud, der fremstod som om, at det kom fra flyselskabet, F. Klageren klikkede på et link i mailen for at betale 80 DKK for køb af en billig flybillet. Hun indtastede sine kortoplysninger og fik efterfølgende sendt en engangskode via SMS til sit telefon- nummer. Efter modtagelse af engangskoden læste klageren teksten i SMS'en. Herefter stoppede hun omgående købet og fik sit kort spærret

I henhold til Kommissionens delegerede forordning 2018/389 af 27. november 2017 artikel 38, stk. 2, trådte kravet om stærk kundeautentifikation (også kaldet to-faktor autentifikation) ved betalingstransaktioner i kraft den 14. september 2019. For så vidt angår kravet til udbydere jf. lov om betalinger § 128, har Finanstilsynet meddelt, at implementering af reglerne for kortbaserede internetbetalinger kan udskydes senest til 31. december 2020, jf. EBA's udtalelse (EBA-Op-2019-11) af 16. oktober 2019 punkt 13. Udsættelsen af implementeringen påvirker imidlertid ikke betydningen af manglende to-faktor autentifikation i forhold til ansvarsreglerne i lov om betalinger, jf. punkt 11 i EBA's nævnte udtalelse. Tilsvarende meddelelse er udsendt af Finanstilsynet.

To-faktor autentifikation indebærer blandt andet, at betalingstjenesteudbydere i forbindelse med godkendelse af kortbaserede internetbetalinger skal forlange, at kunderne bruger minimum 2 ud af 3 mulige sikkerhedselementer (noget kunden ved (fx et kodeord), noget kunden besidder (fx en app eller SMS- engangskode modtaget via et SIM-kort), og noget kunden er (fx et fingeraftryk)), jf. EBA's udtalelse (EBA-Op-2019-06) af 21. juni 2019. Efter det for Ankenævnet oplyste er der ved betalingen, hvor der blev brugt den eksisterende 3DS løsning, ikke anvendt to-faktor autentifikation, idet der er benyttet kortdata og en SMS-engangskode modtaget via et SIM-kort. Da kortdata ikke er hemmelige, men derimod synlige på kortet, udgør de ikke et gyldigt sikkerhedselement, og da SMS-engangskoden sammen med SIM- kortet er noget kunden besidder, opfylder den anvendte betalingssikkerhedsløsning samlet set kun en af de krævede to elementer. Dermed lever den ikke op til kravet om stærk kundeautentifikation.

Tre medlemmer – Bo Østergaard, Ida Marie Moesby og Lisbeth Baastrup Burgaard - udtaler:

Når der ikke er brugt stærk kundeautentifikation, følger det af lov om betalinger § 100, stk. 7, at klageren kun kan komme til at hæfte helt eller delvist for betalingen, jf. lov om betalinger § 100, stk. 3 - 5, hvis klageren har handlet svigagtigt, hvilket der efter sagens oplysninger ikke er grundlag for at antage. Allerede som følge heraf stemmer vi for, at Bank Norwegian skal betale 8.425,49 DKK til klageren.

To medlemmer – Jesper Claus Christensen og Karin Duerlund - udtaler:

Den anvendte SMS-engangskode, der opfyldte kravet til såkaldt "dynamisk linking", jf. lov om betalinger § 128, stk. 2, knyttede betalingstransaktionen til et bestemt beløb og en bestemt betalingsmodtager. Dette var klageren opmærksom på forud for spærringen.

Således som sagen er oplyst for Ankenævnet, er det imidlertid uafklaret, hvordan det har været muligt at gennemføre betalingen, inden klageren spærrede kortet, og der- med også om der foreligger forhold i sagen, som indebærer, at det er uden betydning, at der skulle have været anvendt to-faktor autentifikation ved gennemførelsen af betalingen, eller at der i øvrigt foreligger forhold, der gør, at klageren hæfter, jf. lov om betalinger § 100, stk. 2 og stk. 7.

Vi finder derfor, at en afgørelse af sagen forudsætter en bevisførelse i form af parts-og

vidneforklaringer, der ikke kan ske for Ankenævnet, men i givet fald må finde sted ved domstolene. Vi stemmer derfor for, at Ankenævnet afviser sagen i medfør af Ankenævnets vedtægter § 5, stk. 3, nr. 4.

Der træffes afgørelse efter stemmeflertallet.

Ankenævnets afgørelse

Bank Norwegian skal inden 30 dage til klageren betale 8.425,49 DKK med valør fra datoen for debitering af beløbet.

Klageren får klagegebyret tilbage.