

Finansklagenemnda Bank

Avgjørelse FinKN-2020-505

24.6.2020

SEB Kort Bank AB, Oslofilialen NUF

Betalingsformidling

Omstridte korttransaksjoner – misbruk – phishing?

Saken gjaldt ansvaret for to korttransaksjoner. Klager mottok en e-post med lenke som tilsynelatende var fra Apple i forkant av transaksjonene. Han fulgte lenken og oppga sine kort- og BankID-opplysninger. Banken anførte at kortholderen hadde opptrådt grovt uaktsomt, og at han kunne holdes ansvarlig for en egenandel på kr 12 000. Banken fikk medhold.

ANTATT ØKONOMISK OMFANG: kr 39 900

Saksfremstilling

Saken gjelder ansvaret for to korttransaksjoner på totalt kr 39 990 den 2.10.19 fra klagers MasterCard-konto. Banken opplyser at transaksjonene ble autorisert med BankID samme dag kl. 10.46 og kl. 10.58.

Den 2.10.19 kl. 10.02 mottok klager en e-post med lenke som tilsynelatende var fra Apple. E-posten er fremlagt. I e-posten ble det opplyst om at klagers AppleID ble brukt til å logge inn på iCloud fra en IP-adresse i Shanghai. Klager ble anmodet om å følge lenken i e-posten hvis det ikke var ham selv som hadde logget inn. Klager fulgte lenken og oppga sine kort- og BankID-opplysninger.

Klager ble kontaktet av banken som informerte ham om de to omstridte transaksjonene. Klager ba deretter banken om å sperre kortet. Banken opplyser at kortet ble sperret kl. 11.30.

Klager har anført at han ikke kan holdes ansvarlig for en egenandel på kr 12 000. Han erkjenner å ha utvist uaktsomhet, men derimot ikke at han opptrådte grovt uaktsomt. Klager ble skremt av at noen i Kina hadde fått tilgang til hans konto, og han ble nok stresset av det. Klager har ikke hatt til hensikt eller oppfattet det som at han kan ha bidratt til godkjenning av kjøp av varer. Som en helt alminnelig kortbruker fra midten av 80-tallet, tenkte han ikke umiddelbart på svindel da han mottok e-posten. E-posten liknet på slike meldinger man får fra Apple når ny telefon eller nettbrett tas i bruk, og klager oppfattet derfor e-posten som troverdig. Klager var ikke kjent med at det var advart mot denne typen svindel. På bakgrunn av forannevnte krever klager at banken kompenserer ham for hele tapet.

Finansforetaket har anført at transaksjonene ble autorisert kort tid etter at klager mottok e-posten og før han fikk sperret kortet. Det må derfor kunne legges til grunn at klager har oppgitt kort- og BankID-opplysninger etter å ha fulgt lenken i e-posten, før han var i kontakt med banken. Det har både blitt advart generelt mot phishing-svindel og mer spesielt mot Apple-phishing, og nemnda har vanligvis konkludert med grov uaktsomhet i disse sakene. Avsenderadressen i e-posten var lite troverdig. Det er heller ingen naturlig sammenheng mellom å skifte passord for en Apple-konto og å skulle oppgi kort- og BankID-opplysninger. De forannevnte momentene tilsier at

klager må anses for å ha opptrådt grovt uaktsomt. Klager må derfor kunne holdes ansvarlig for kr 12 000 av tapet.

Finansklagenemnda Banks begrunnelse

Banken anfører at kortholderen (klageren) har opptrådt grovt uaktsomt, og at han derfor kan holdes ansvarlig for en egenandel på kr 12 000 i medhold av finansavtalel. § 35 tredje ledd. Kortholderen forklarer at han fant e-posten troverdig. Den ligner på slike meldinger som man får fra Apple når en ny telefon eller et nytt nettbrett tas i bruk. Han forklarer videre at han var stresset over situasjonen som var oppstått. Slik nemnda forstår klagerens forklaring, bestrider han ikke å ha fulgt lenken i e-posten og deretter oppgitt sine kort- og BankID-opplysninger på det nettstedet han ble ledet til.

Nemnda har i sin tidligere praksis i saker om "phishing" vist til at det jevnlig advares mot falske e-poster og tekstmeldinger som tilsynelatende kommer fra kjente avsendere, og som inneholder lenker til sider hvor mottakeren blir bedt om å gi kortnummer og sikkerhetsopplysninger, herunder sikkerhetsdata for BankID. Nemnda antar at advarsler mot å følge lenker og å gi sikkerhetsopplysninger er allment kjente. I nemndas tidligere praksis har det i de fleste sakene vært ansett grovt uaktsomt å følge slike lenker og å gi opplysninger. Det er likevel påpekt at vurderingen av kortholderens grad av skyld må foretas ut fra sakens individuelle omstendigheter. Det finnes i nemndas praksis flere saker hvor nemnda, enstemmig eller under dissens, på grunn av sakens spesielle omstendigheter har konkludert med at vilkåret om grov uaktsomhet ikke var oppfylt.

Nemnda kan ikke se at det foreligger slike spesielle omstendigheter i denne saken. Selv om nemnda kan ha forståelse for at man kan bli stresset av å motta en e-post som denne, vil det etter nemndas syn være grovt uaktsomt å gi fra seg kort- og sikkerhetsopplysninger uten å foreta en nærmere vurdering av e-postens ekthet og troverdighet. Adressen app@rep.com som e-posten kom fra, fremstår etter nemndas syn som lite tillitvekkende. Innholdet i e-posten var en anbefaling om å skifte passord for klagerens iCloud-konto. Opplysninger om betalingskort og bekreftelse med BankID er ikke en naturlig del av prosess med skifte av passord. Med den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle, mener nemnda det må regnes som grovt uaktsomt å la seg svindle på denne måten. Nemnda konkluderer med at kortholderen har opptrådt grovt uaktsomt i saken, og at han derfor er ansvarlig for den egenandelen på kr 12 000 som kortholderen må dekke ved grov uaktsomhet.

Avgjørelsen er enstemmig.

Finansklagenemnda Banks konklusjon

Banken gis medhold.

Ved behandlingen deltok Trygve Bergsåker (leder), Tom Slungaard (selskapsrepresentant) og Kristoffer Sørli (forbrukerrepresentant).