Finansklagenemnda Bank

Avgjørelse FinKN-2018-311

3.5.2018

EnterCard Norge, filial av EnterCard Group AB

Betalingsformidling (bl.a. misbruk av betalingskort)

Uautorisert belastning på konto — svindel — phishing.

Kortholder ble utsatt for svindel i form av phishing. Hun ble kontaktet angivelig av Nets og bedt om å gi diverse opplysninger for å få åpnet kortet som angivelig var sperret. Kontoen ble deretter belastet for kr 9 412 til selskapet Free Mobile i Frankrike. Kortholder hadde tidligere samme dag forsøkt å kontakte sperretjenesten for å sperre kortet uten at hun oppnådde kontakt. Nemnda har tidligere konkludert med at det er grovt uaktsomt å oppgi kortdata og personlige sikkerhetsanordninger ved å følge lenker i e-postmeldinger hvor det bes om slike. Dette gjelder selv om e-postmeldingen tilsynelatende kommer fra en seriøs aktør og er profesjonelt utført. Her foreligger spesielle omstendigheter som gjør at nemnda ikke finner kortholders handlemåte å være grovt uaktsom.

ANTATT ØKONOMISK OMFANG: kr 9 412

Saksfremstilling

Klagen er bragt inn av kortholder.

Saken gjelder ansvaret for en uautorisert belastning på kortholders kredittkonto etter at hun ble utsatt for svindel.

Kortholder mottok 15.10.17 en e-postmelding fra noen som utga seg for å være fra IT-selskapet Nets. Hun ble informert om at kortet var sperret, og at hun kunne åpne kortet ved å taste på en lenke og deretter følge anvisningen i e-postmeldingen. Kortholder opplyste at hun tidligere på dagen hadde gjort flere forsøk på å sperre kortet, etter at hun skal ha glemt det igjen i en kiosk. Kortholder ringte både nummeret som fremgikk av mobilappen for COOP MasterCard og nummeret som fremgikk av EnterCards internettsider. Kortholder fikk begge gangene informasjon om at sperretjenesten var stengt, noe hun antok skyldtes at det var helg, og hun ga til slutt opp. Da kortet kom til rette, kort tid før hun mottok svindel e-postmeldingen, antok hun at hun likevel hadde klart å sperre kortet, og at hun kunne åpne det igjen ved å følge anvisningen i e-postmeldingen. Kortholder fulgte lenken som fremkom av e-postmeldingen, og la deretter inn kortnummeret og CVC-nummeret. I tillegg oppga hun telefonnummeret, slik at svindlerne etter det de opplyste til henne, kunne sende henne en kode som hun skulle benytte for å bekrefte åpningen av kortet. Kortholder tastet deretter inn koden som hun mottok på SMS, på den falske internettsiden. EnterCard har dokumentert at belastningen er gjennomført ved bruk av 3DSecure-passord.

EnterCard er kjent med at det har blitt sendt ut slike e-postmeldinger hvor kortholder informeres om at kort eller konto er sperret, og at man må ta nødvendige grep for å få åpnet disse igjen.

Kortholder fikk mistanke om at hun var blitt utsatt for svindel da hun oppdaget at kontoen var belastet med et beløp på kr 9 412. Beløpet er gått til selskapet Free mobile i Frankrike.

Klager bestrider å ha opptrådt grovt uaktsomt. Hun bestrider å ha tastet inn andre koder en den hun fikk på SMS av svindlerne. Hun handlet i god tro og oppdaget ikke at hun var utsatt for svindel. I og med at hun tidligere på dagen hadde forsøkt å sperre kortet, hadde hun tiltro til at henvendelsen faktisk kom fra Nets og at hun hadde klart å sperre kortet. Da kortet samtidig var kommet til rette, benyttet hun muligheten til å åpne kortet igjen ved å svare på e-postmeldingen. Kortholder anser at EnterCard må stå ansvarlig for belastningen fordi sperretjenesten ikke fungerte.

Finansforetaket anser at kortholder er blitt utsatt for kortmisbruk kalt "phishing". Finansforetaket har anført at kortholder har unnlatt å oppfylle sine forpliktelser etter kortkontrakten ved å gjøre kortinformasjon og kode og personlig passord tilknyttet sin BankID tilgjengelig for uvedkommende. Advarsler mot å følge slike lenker i e-postmeldinger og SMS antas å være allment kjent. Kortholder anses for å ha opptrådt grovt uaktsomt og må dermed stå ansvarlig for inntil kr 12 000 av det omstridte beløp, i dette tilfelle kr 9 412.

EnterCard anser at det beror på en tilfeldighet at svindel-eposten kom samme dag som hun forsøkte å sperre kortet.

EntarCard bekrefter at det finnes to ulike telefonnummer man kan ringe for å sperre et kort, både ett som fremkommer i mobilappen for COOP MasterCard, samt et annet som fremkommer av EnterCards nettsider. Telefonnummeret som oppgis i mobilappen lå nede den aktuelle helgen på grunn av teknisk feil. Telefonnummeret som oppgis på EnterCards nettsider var åpent og tilgjengelig. Begge numre tilhører Nets, som leverer EnterCards sperretjenester. Nets har ikke registrert noen kontakt fra kortholder den datoen hun forklarte at hun forsøkte å sperre kortet.

EnterCard anser at det er flere logiske brister i kortholders forklaring om hendelsesforløpet.

Finansklagenemnda Banks begrunnelse

Det følger av finansavtalel. § 35 første ledd at banken i utgangspunktet er ansvarlig for tap som skyldes uautorisert betalingstransaksjon. Dersom tapet skyldes at kortholderen grovt uaktsomt har unnlatt å beskytte personlige sikkerhetsanordninger knyttet til kortet, er kortholderen ifølge § 35 tredje ledd, jf. § 34 første ledd, ansvarlig for en egenandel på kr 12 000. Det beløpet som er belastet kortet i denne saken, ligger innenfor denne egenandelen. Kortholderen er ifølge § 35 annet ledd uansett ansvarlig for en egenandel på kr 1 200 når han eller hun har mislyktes i å beskytte personlige sikkerhetsanordninger.

Kortholderen ble lurt til å oppgi kortdata og personlige sikkerhetsanordninger etter å ha mottatt en e-post som tilsynelatende kom fra Nets. I e-posten ble det opplyst at kortet var sperret, og det ble beskrevet en prosedyre for å åpne det igjen. Kortholderen forklarer at hun tidligere samme dag hadde forsøkt å sperre kortet fordi hun hadde lagt det igjen i en kiosk. Hun oppnådde ikke kontakt med sperretjenesten. Det er bekreftet at det var problemer med sperretjenesten i det aktuelle tidsrommet. Før hun mottok den nevnte e-posten, hadde hun oppsøkt kiosken og fått kortet tilbake. Da hun fikk e-posten, oppfattet det slik at kortet var blitt sperret. Hun fulgte lenken i e-posten for å oppheve sperringen. I denne prosessen oppga hun kort- og sikkerhetsdata som gjorde svindelen mulig.

Nemnda har i tidligere saker lagt til grunn at det er grovt uaktsomt å oppgi kortdata og personlige sikkerhetsanordninger ved å følge lenker i eposter som ber om slike opplysninger. Dette gjelder selv om e-posten tilsynelatende kommer fra en seriøs aktør og er så profesjonelt utført at den virker troverdig. I denne saken er omstendighetene spesielle ved at kortholderen tidligere samme dag hadde forsøkt å sperre kortet, og ved at e-posten kom fra Nets, som kunne oppfattes som rett instans for en henvendelse om sperringen. Nemnda er i lys av sakens spesielle omstendigheter

kommet til at det ikke er grunnlag for å konkludere med grov uaktsomhet fra kortholderens side. Kortholderens ansvar er begrenset til egenandel på kr 1 200 etter § 35 annet ledd.

Avgjørelsen er enstemmig.

Finansklagenemnda Banks konklusjon

Kortholderen er ansvarlig for en egenandel på kr 1 200.

Ved behandlingen deltok Trygve Bergsåker (leder), Monica Viken (nestleder), Monica M. Zak (nøytralt oppnevnt medlem), Erik Bøhn (selskapsrepresentant), Jan Fr. Haraldsen (selskapsrepresentant), Ane Køber Opstad (forbrukerrepresentant) og Gyrid Giæver (forbrukerrepresentant).