Finansklagenemnda Bank

Avgjørelse FinKN-2019-039

18.1.2019

DNB Bank ASA

AZ - Betalingsformidling (bl.a. misbruk av betalingskort)

Svindel – phishing – trodde han betalte faktura til Apple.

Kortholder ble utsatt for svindel i form av phishing. Han fulgte en lenke som tilsynelatende kom fra Apple hvor det sto at han skyldte penger, for å betale. En belastning på kr 11 397 som klager ikke vedkjenner, seg ble foretatt til Klarna. Nemnda legger til grunn at kortholder gav fra seg sikkerhetsopplysningene da han tastet sin BankID, og at disse ble fanget opp av svindlerne og misbrukt. Dette anses å være grovt uaktsomt av kortholder, i betraktning av den omfattende publisitet tilsvarende saker har fått i mediene. Kortholder kan holdes ansvarlig for det omstridte beløp.

ANTATT ØKONOMISK OMFANG: kr 11 391

Saksfremstilling

Saken gjelder ansvarsforhold etter misbruk av kortdetaljer knyttet til kortholders Leve Visakort utstedt av DNB.

Klager opplyser at han 17.7.18 mottok en e-post fra noen som utga seg for å være fra Apple. Det sto i e-postmeldingen at han skyldte Apple penger. I e-postmeldingen var det inntatt en lenke, som klager fulgte for å betale. I den forbindelse la han inn betalingsinformasjon og legitimerte seg med BankID. Det er ikke opplyst hva klager angivelig skyldte Apple. Klager oppdaget at en belastning på kr 11 397 var gått til Klarna klarmobil GmbH i Budelsdorf, Tyskland, kl. 11.03. Belastningen er autorisert med klagers BankID. Klager fikk mistanke om at det dreide seg om svindel og kontaktet banken for å få pengene tilbake.

Klager bestrider å ha autorisert transaksjonen. Han har ikke opptrådt grovt uaktsomt. Han ble lurt til å tro at e-posten kom fra Apple og fulgtet lenken for å betale regningen. Klager hadde ikke mistanke om at den var falsk, da e-posten så svært ekte ut. Klager er usikker på hvordan svindelen har foregått.

Finansforetaket anser at klager har opptrådt grovt uaktsomt, og dermed kan holdes ansvarlig for en egenandel på kr 12 000, i dette tilfellet hele beløpet. For at svindlerne skal kunne foreta belastningen, må de ha fått tilgang til kortopplysningene og passordet til klagers BankID. Banken viser til tidligere nemndspraksis, blant annet FinKN-2017-649 hvor det konkluderes med at klager har opptrådt grovt uaktsomt ved å følge lenken i e-posten i stedet for selv å taste inn e-postadressen og deretter legge inn sikkerhetsopplysninger.

Finansklagenemnda Banks begrunnelse

Spørsmålet i saken er om kortholderen grovt uaktsomt har unnlatt å beskytte sine personlige sikkerhetsanordninger for kortet, med den konsekvens at han etter finansavtalel. § 35 tredje ledd,

jf. § 34 første ledd, er ansvarlig for en egenandel på kr 12 000. Den aktuelle personlige sikkerhetsanordningen som kan være røpet, er kortholderens BankID.

Det er ikke full enighet om hendelsesforløpet i saken. Det er enighet om at kortholderen fikk en e-post som tilsynelatende kom fra Apple. Denne e-posten inneholdt lenke til en Apple nettside. Både e-posten og den nettsiden den ledet til, var falske. Det er ikke enighet om hvilke opplysninger kortholderen la igjen på den falske Apple-siden. Han benekter tilsynelatende å ha tastet sin BankID på den falske nettsiden. På den annen side forklarer han at han betalte det beløpet han ble opplyst å skylde. Det er noe uklart om kortholderen mener å ha betalt dette i sin nettbank eller på den falske nettsiden han ble ledet inn på. Nemnda kan ikke betvile bankens opplysning om at den omtvistede belastningen ble gjennomført som kortbetaling, og at den ble autorisert med engangskode og personlig passord fra kortholderens BankID.

Kortholderen har ikke lagt frem den e-posten han fikk og som inneholdt lenken. Heller ikke har kortholderen besvart et spørsmål under saksforberedelsen om størrelsen på det beløpet han ble bedt om å betale, og som han etter egen forklaring også betalte til Apple. Nemnda forstår det slik at den betalingen han forklarer å ha foretatt, er en annen enn den som er omtvistet i saken.

Nemnda vil vise til at det jevnlig advares mot falske e-poster som tilsynelatende kommer fra kjente avsendere, og som inneholder lenker til sider hvor mottakeren blir bedt om å gi kortnummer eller sikkerhetsopplysninger knyttet til betalingskort. Nemnda antar at advarsler mot å følge lenker og å gi sikkerhetsopplysninger er allment kjente. I nemndas tidligere praksis har det vært ansett grovt uaktsomt å følge slike lenker og å gi opplysninger. Vurderingen av kortholderens grad av skyld må likevel foretas ut fra sakens individuelle omstendigheter. Det finnes i nemndas nyere praksis i hvert fall ett eksempel (FinKN-2018-311) på at nemnda, på grunn av sakens helt spesielle omstendigheter, har konkludert med at vilkåret om grov uaktsomhet ikke var oppfylt. Slike spesielle omstendigheter foreligger ikke i den saken som nå er til behandling.

Kortholderen fulgte en lenke i en e-post i stedet for selv aktivt å taste inn nettadressen, og han ga fra seg sikkerhetsopplysninger på den nettsiden som lenken førte ham til. Med den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle, mener nemnda at det må det regnes som grovt uaktsomt å gi sikkerhetsopplysninger på denne måten. Nemnda konkluderer med at kortholderen har opptrådt grovt uaktsomt i saken. Nemnda mener etter dette at tapet skyldes at kortholderen ved grov uaktsomhet har unnlatt å beskytte sine personlige sikkerhetsanordninger. Belastningen ligger innenfor den egenandelen på kr 12 000 som kortholderen må dekke ved grov uaktsomhet.

Nemnda vil avslutningsvis bemerke at en transaksjon som er reservert på kortkontoen til fordel for et brukersted i kraft av en tilsynelatende gyldig autorisasjon, ikke kan stoppes av banken etter instruks fra kortholderen.

Avgjørelsen er enstemmig.

Finansklagenemnda Banks konklusjon

Kortholderen kan holdes ansvarlig for den omtvistede kortbelastningen på kr 11 391.

Ved behandlingen deltok Trygve Bergsåker (leder), Ingvild Dønnem Søyseth (selskapsrepresentant), Henning Bjørnstad (selskapsrepresentant), Gyrid Giæver (forbrukerrepresentant) og Helene Folmo Hafnor (forbrukerrepresentant).