Finansklagenemnda Bank

Avgjørelse FinKN 2021-838

13.9.2021

Sbanken ASA

Betalingsformidling

Omstridte betalingstransaksjoner – Apple-phishing.

Saken gjaldt ansvaret for flere betalingstransaksjoner gjennomført med klagers BankID-opplysninger. Klager opplyste at han hadde blitt oppringt av noen som utga seg for å være fra Apple. Han oppga sine kort- og BankID-opplysninger. Klager mente at han ikke hadde vært grovt uaktsom. Banken anførte at klager måtte holdes ansvarlig for en egenandel på kr 12 000. Banken fikk medhold.

ANTATT ØKONOMISK OMFANG: kr 12 000

Saksfremstilling

Saken gjelder spørsmålet om hvorvidt banken kan holde klager ansvarlig for en egenandel på kr 12 000 etter at han ble utsatt for svindel.

Klager fikk 9.2.2021, mens han var på hjemmekontor, en telefonoppringning fra noen som utga seg for å være fra Apple. Vedkommende opplyste at klagers Mac var hacket, og at klager selv kunne se dette ved å logge seg inn på apple.com. Klager opplyser at han ble ledet gjennom et program som svindleren opplyste skulle slette den trojanske hesten, noe som tok 30-40 minutter. Klager ble etter hvert utålmodig og ville overlate arbeidet til en datakyndig på arbeidsplassen. Vedkommende svarte at da var alt arbeidet forgjeves, og at de ikke hadde tid til å hjelpe en gang til.

Klager aksepterte tilbudet om kjøp av en brannmur til kr 25 slik at viruset ikke fikk spredt seg videre. Klager opplyste at fakturaen han mottok så troverdig ut. Klager betalte for brannmuren ved å legge inn kortnummer og bekreftet betalingen med BankID på mobil. Betalingen ble ikke bekreftet første gang, og klager gjentok betalingsprosessen én eller to ganger til før den gikk igjennom. Klager har videre forklart at han oppgav sin BankID på mobil for å identifisere seg.

Klager har forklart at han oppdaget svindelen da han så transaksjonene på kontoen og ringte banken. Det ble gjennomført i alt fem transaksjoner på totalt kr 32 983. Betalingene ble gjennomført ved bruk av kortopplysningene i klagers Visa-kort og bekreftet med 3DSecure og BankID. Betalingene gikk til Transferwise Ltd. Kortet ble sperret 9.2.21 kl. 13.03.

Klager bestrider å ha opptrådt grovt uaktsomt. Klager har ikke oppført seg annerledes enn det han vanligvis gjør. Det svindleren sa virket svært troverdig, og klager hadde ikke mistanke om at det dreiet seg om svindel. I og med at det var et lite beløp tok han sjansen. Hadde klager ikke hatt hjemmekontor, ville han ikke blitt svindlet. Klager anser at det er et hull i bankens Visas-systemer.

Finansforetaket anser at klager er blitt utsatt for kortmisbruk kalt "phishing". Svindlerne fikk tilgang til klagers Mac ved at han tastet på en lenke og lot den fjernstyres. Banken viser til at det er lite sannsynlig at Apple skulle opptre slik svindlerne gjorde i dette tilfellet. Klager hadde heller

ingen forsikring for at personen i telefonen faktisk var den han utga seg for å være. Når personen i telefonen gir instrukser som leder frem til at strengt personlig betalingsinformasjon må oppgis, må det anses som grovt uaktsomt å etterkomme disse instruksene. Ifølge kortavtalen og finansavtaleloven § 35 tredje ledd svarer klager for en egenandel på kr 12 000 av tapet. Banken viser til at den ikke har mulighet til å stoppe en transaksjon, uten fullmakt fra brukerstedet, fra og med det tidspunktet kortholder autoriserer beløpet ved hjelp av engangspassordet på SMS.

Finansklagenemnda Banks begrunnelse

Saken gjelder spørsmålet om kortholderen kan belastes egenandel på kr 12 000 etter fem uautoriserte transaksjoner på hans betalingskort 9.2.21 på til sammen kr 32 983.

Partene er enige om at de omtvistede transaksjonene ikke er autorisert av kortholderen. Betalinger som ikke er autorisert av kortholderen, er i utgangspunktet bankens ansvar etter finansavtalel. § 35 første ledd. I § 35 tredje ledd finnes flere unntak fra utgangspunktet i første ledd. Av tredje ledd andre punktum følger det at kortholderen er ansvarlig for egenandel på kr 12 000 dersom han ved grov uaktsomhet har unnlatt å oppfylle sine plikter etter finansavtalel. § 34 første ledd. Pliktene etter § 34 første ledd omfatter blant annet å beskytte de personlige sikkerhetsanordningene som er knyttet til betalingskort. Banken anfører at kortholderen har opptrådt grovt uaktsomt, og at han derfor kan holdes ansvarlig for en egenandel på kr 12 000.

Kortholderen mener at han ikke har opptrådt grovt uaktsomt, og at han derfor ikke kan holdes ansvarlig for egenandel. Han fant situasjonen troverdig og hadde ingen grunn til mistanke om at telefonoppringningen var falsk og ledd i svindel. Siden beløpet på kr 25 som han ble bedt om å betale var så lite, så han ingen betenkelighet ved å betale dette. Han forklarer at han måtte taste kort- og BankID-opplysninger flere ganger før betalingen gikk gjennom. Deretter måtte han bekrefte sin identitet ved å taste sin BankID nok en gang. Heller ikke dette lyktes første gangen og måtte derfor gjentas. Det er ingen uenighet om at de omtvistede betalingene ble gjennomført med kortholderens visakort og bekreftet med hans BankID på mobil. Svindelen har latt seg gjennomføre ved at svindleren har kunnet nyttiggjøre seg de sikkerhetsopplysningene som kortholderen oppga gjentatte ganger.

Nemnda har i sin tidligere praksis i saker om "phishing" vist til at det jevnlig advares mot falske e-poster, tekstmeldinger og telefonoppringninger som tilsynelatende kommer fra kjente avsendere, og hvor mottakeren blir bedt om å gi fra seg kortnummer og sikkerhetsopplysninger gjennom lenker eller på annen måte. Nemnda antar at advarsler mot å følge slike anmodninger og å gi fra seg 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. Kortholderen forklarer at han ga fra seg sikkerhetsopplysninger flere ganger, siste gang angivelig for å bekrefte sin identitet. Svindleren kunne nyttiggjøre seg opplysningene til å belaste betalingskortet i alt fem ganger. Det er opplyst at svindleren hadde tilgang til kortholderens PC. Kortholderen forklarer at han satt på hjemmekontor, og at han på et tidspunkt i samtalen med svindleren ville overlate problemløsningen til IT-hjelp på arbeidsplassen. I lys av dette fremstår det for nemnda som rart at han aksepterte kjøp av brannmur privat av Apple, selv om beløpet var lite.

Den situasjonen som kortholderen beskriver var etter nemndas syn så spesiell at nemnda mener at kortholderen har opptrådt grovt uaktsomt ved å oppgi kortopplysninger og taste inn sikkerhetsopplysninger fra sin BankID på mobil. Han kan holdes ansvarlig for egenandel på kr 12 000 som kortholderen må dekke ved grov uaktsomhet.

Nemnda vil for ordens skyld bemerke at banken ikke kan stanse en korttransaksjon som tilsynelatende gyldig autorisert selv om beløpet i første omgang står som reservert på kontoen.

Avgjørelsen er enstemmig.

Finansklagenemnda Banks konklusjon

Banken gis medhold.

Ved behandlingen deltok Trygve Bergsåker (leder), Carl Håkon Andersen (selskapsrepresentant) og Caroline Skarderud (forbrukerrepresentant).