

Finansklagenemnda Bank

Avgjørelse FinKN-2020-19

13.1.2020

Bjugn Sparebank

Betalingsformidling (bl.a. misbruk av betalingskort)

Svindel – phishing – e-post fra Apple – hadde utvidet lagringskapasiteten noen uker i forveien.

Klager ble svindlet etter å ha mottatt en e-post som fremsto som om den kom fra Apple. Klager fulgte en lenke for å avbestille en skytjeneste hun fikk opplyst at hun hadde kjøpt. Klager hadde gjennomført en utvidelse av lagringskapasiteten i skytjenesten Apple iCloud noen uker i forveien. Klager bekreftet at hun hadde tastet inn kortopplysningene men bestred å ha benyttet BankID. Spørsmålet i saken var om kortholderen grovt uaktsomt hadde unnlatt å beskytte sine personlige sikkerhetsanordninger for kortet, med den konsekvens at hun etter finansavtalel. § 35 tredje ledd, jf. § 34 første ledd, var ansvarlig for en egenandel på kr 12 000. Kortholder fikk medhold. Avgjørelsen ble gitt under dissens.

ANTATT ØKONOMISK OMFANG: kr 12 000

Saksfremstilling

Saken gjelder ansvaret for tap etter at klager ble utsatt for svindel.

Klager mottok 10.1.19 en e-post fra noen som utga seg for å være fra Apple. Klager ble informert om at hun var trukket kr 599 til betaling for en tjeneste i iCloud, som hun kunne avbestille ved å taste på lenken på fakturaen. Da den oppgitte lagringsmengden (2 TB) i den falske fakturaen var uventet høy, valgte kortholder å følge lenken for å avbestille. Hun kom deretter inn på en side hun syntes så helt lik ut som hennes Apple-side. Klager la deretter inn kortopplysningene. Klager bestrider at hun benyttet BankID. Klager hadde utvidet lagringskapasiteten i skytjenesten Apple iCloud noen uker i forveien. Ettersom slik utvidelse faktureres månedlig av Apple via e-post, ble den falske e-posten sett i sammenheng med denne forutgående endringen av lagringskapasitet.

Hun så at kontoen var belastet 10.1.19 kl. 20.02 med et beløp på kr 15 433 til fordel for Reichelt Elektronik i Tyskland. Klager kontaktet banken og fikk sperret kortet. Hun kontaktet samtidig den tyske nettbutikken "Reichelt Elektronik" for å få kansellert svindelbestillingen og refundert betalingen. Ettersom nettbutikken allerede morgenen etter svindelen hadde sendt ut varen som var bestilt, kunne ikke bestillingen kanselleres. Videre nektet nettbutikken av personvern hensyn å gi opplysninger om hvem som hadde utført bestillingen.

Klager har dokumentert at hun hadde medlemskap i Apple, samt hadde utvidet lagringskapasiteten på tidspunktet for svindel-e-posten.

Klager bestrider å stå ansvarlig for transaksjonen. Hun var i god tro. Klager ble lurt til å tro at e-posten kom fra Apple, da hun kun noe uker i forveien hadde utvidet sin lagringskapasitet i iCloud. Klager reagerte dermed ikke på opplysningen om at hun var blitt belastet for denne tjenesten. Klager hadde ikke mistanke om at den var falsk, da e-posten så svært ekte ut og identisk med den hun vanligvis får fra Apple på e-post hver måned. Da den oppgitte lagringsmengden (2 TB) i den falske fakturaen var uventet høy, valgte kortholder å følge lenken for å avbestille. Det var ikke

dårlig norsk eller andre signaler som kunne indikere at den var falsk. Klager bestrider å ha benyttet BankID.

Finansforetaket anser at klager må stå ansvarlig for belastningen. Banken har dokumentert at transaksjonen er bekreftet med BankID. Kortet har en kredittramme på kr 30 000, som ikke var overskredet i forbindelse med belastning av den gjeldende transaksjonen. Svindelmetoden som her er benyttet er allment kjent og det var dermed grovt uaktsomt av klager å ikke gjennomskue den.

Finansklagenemnda Banks begrunnelse

Spørsmålet i saken er om kortholderen (klageren) grovt uaktsomt har unnlatt å beskytte sine personlige sikkerhetsanordninger for kortet, med den konsekvens at hun etter finansavtalel. § 35 tredje ledd, jf. § 34 første ledd, er ansvarlig for en egenandel på kr 12 000. Den omtvistede transaksjonen er ifølge bankens logg bekreftet med kortholderens BankID. Kortholderen mener selv at hun la inn opplysningene som står på betalingskortet, men at hun ikke brukte sin BankID på den falske siden. Nemnda forstår det slik at partene er enige om at den omtvistede transaksjonen er utført av uvedkommende, og at den ble muliggjort som følge av de opplysningene kortholderen la inn på den falske siden. Når bankens logg viser at transaksjonen ble bekreftet med kortholderens BankID, må nemnda legge til grunn at kortholderen benyttet denne, muligens uten at hun selv husker det i ettertid.

Nemnda vil vise til at det jevnlig advares mot falske henvendelser i form av telefonoppringninger, e-poster og tekstmeldinger som tilsynelatende kommer fra kjente avsendere, og hvor mottakeren anmodes om å foreta handlinger som innebærer at svindleren får tilgang til sikkerhetsopplysninger knyttet til betalingskort eller konti. Nemnda antar at advarsler mot å følge slike henvendelser er allment kjente. I nemndas tidligere praksis har det i mange tilfeller vært ansett grovt uaktsomt å gi eller røpe sikkerhetsopplysninger etter slike henvendelser. Vurderingen av kortholderens grad av skyld må likevel 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 (FinKN-2018-311, FinKN-2019-336, FinKN-2019-338, FinKN-2019-619, FinKN-2019-800, FinKN-2019-803).

Nemndas flertall, bestående av Trygve Bergsåker, Gyrid Giæver og Paal Bjønness, bemerker:

Nemndas flertall er kommet til at kortholderen i denne saken må gis medhold, og at hun ikke kan holdes ansvarlig for en egenandel på kr 12 000. Kortholderen forklarer at hun koblet den falske fakturaen fra Apple til en oppgradering med ekstra lagringsplass for bilder i iCloud som hun nylig hadde foretatt, og at hun derfor ikke hadde mistanke om at fakturaen kunne være falsk.

Den falske fakturaen er lagt frem for nemnda, og flertallet mener at den virker troverdig, selv om den avviker noe fra en ekte faktura fra Apple. Man kan stusse på at fakturaen skulle ha en lenke for å avbryte ordren, men dette er etter flertallets syn i seg selv ikke så påfallende og mistenkelig at kortholderen klart burde ha innsett at e-posten og fakturaen kunne være falsk.

Terskelen for grov uaktsomhet må vurderes ut fra det livsområdet saken gjelder. At kortholderen kan bebreides for manglende påpasselighet, er uansett ikke tilstrekkelig til å konkludere med grov uaktsomhet. Skyldgraden må vurderes ut fra publikums vanlige forutsetninger og erfaringer. Ut fra den forklaringen som kortholderen har gitt om bakgrunnen for at hun oppfattet e-posten som troverdig, kan flertallet ikke konkludere med at vilkåret om grov uaktsomhet er oppfylt. Kortholderen kan etter dette ikke belastes egenandel på kr 12 000.

Nemndas mindretall, Trond A. Lie og Ingvild D. Søyseth, bemerker:

Mindretallet har kommet til at kortholder ikke kan gis medhold, og at hun er ansvarlig for en egenandel på kr 12 000. Nemndas mindretall finner at det i denne saken ikke foreligger slike spesielle omstendigheter at det kan konkluderes med at kortholderen ikke har utvist grov uaktsomhet.

Med den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle ved blant annet å følge lenker i tilsendte e-poster, mener nemndas mindretall at det må det regnes som grovt uaktsomt å gi fra seg kortopplysninger og sikkerhetsopplysninger i denne saken.

Når det gjelder fakturaen kan den i utgangspunktet fremstå som troverdig, men det er likevel forhold ved den som innebærer at den skiller seg fra en ekte faktura fra Apple. For øvrig er heller ikke prosedyre for betaling/kjøp og administrasjon av Apple-konto i samsvar med Apples praksis.

Når det gjelder administrasjon av Apple-konto, ved for eksempel betaling/kjøp og oppdatering av kontoinformasjon, gjøres dette via innlogging på personlig konto. Apple-brukeren legger inn betalingsinformasjon, og kjøp blir deretter foretatt via den personlige Apple-kontoen. Apple sender ikke ut e-post med lenke til betaling eller for å oppdatere betalingsinformasjon i tilknytning til Apple-kontoen. Dersom Apple-brukeren har foretatt et kjøp, sender Apple i etterkant ut faktura. Denne inneholder informasjon om kjøpet som er foretatt. Det nevnes for øvrig at fakturaen inneholder fakturaadressen til Apple-brukeren, hvilket fakturaen i denne saken ikke gjorde. Informasjon om hvordan svindel kan unngås er tilgjengelig på Apples hjemmeside.

Prosedyren kortholder ble bedt om å følge i denne saken er dermed ikke i samsvar med vanlig prosedyre for administrasjon og bruk av Apple-konto. Videre er det i seg selv svært mistenkelig å motta en lenke for å avbryte en ordre. Det er heller ikke i samsvar med vanlig praksis for avbestilling av ordrer ellers.

I denne saken har kortholderen trykket på en lenke i den hensikt å avbestille, før hun uten plausibel grunn gir fra seg både kortnummer og CRV-kode. Det er kombinasjonen av at kortholderen har oppgitt kortinformasjon sammen med data fra BankID som utløser tapet i saken. På bakgrunn av ovennevnte mener mindretallet etter dette at tapet skyldes at kortholder ved grov uaktsomhet har unnlatt å beskytte sine personlige sikkerhetsanordninger.

Avgjørelsen er avgitt under dissens.

Finansklagenemnda Banks konklusjon

Kortholderen gis medhold.

Ved behandlingen deltok Trygve Bergsåker (leder), Trond A. Lie (selskapsrepresentant), Ingvild Dønnem Søyseth (selskapsrepresentant), Gyrid Giæver (forbrukerrepresentant) og Paal Bjønness (forbrukerrepresentant).