

Finansklagenemnda Bank

Avgjørelse FinKN 2021-544

2.6.2021

Storebrand Bank ASA

Betalingsformidling

Uautoriserte betalingstransaksjoner – svindel – opplyst sikkerhetsopplysninger til en person som utga seg for å være ansatt i banken – samtykket til transaksjonen? – forsett? – grov uaktsomhet?

Klager mottok en svindel-sms på en meldingstråd der han også hadde mottatt autentiske sms'er fra Storebrand. Svindel-sms'en opplyste om nye pålagte sikkerhetskrav for Storebrand, og at klager ville motta en sikkerhetskode for sterk kundeautentisering. Klager ble kort tid etterpå oppringt av en person som utga seg for å jobbe i Storebrands kryptoavdeling. Klager oppga koden på forespørsel fra personen i telefonen. Etter at samtalen var avsluttet mottok klager flere oppringninger fra et ukjent nummer og et varsel om at mobilbank var i ferd med å bli registrert på en ukjent enhet. Fire dager senere ble det gjennomført to transaksjoner fra klagers nettbank som klager ikke vedkjente seg. Banken anførte prinsipalt at klager hadde samtykket til transaksjonene, subsidiært at klager forsettlig hadde utlevert sine personlige sikkerhetsopplysninger, og atter subsidiært at klager hadde opptrådt grovt uaktsomt. Saken ble avvist fra behandling ved Finansklagenemnda.

ANTATT ØKONOMISK OMFANG: kr 228 012

Saksfremstilling

Saken gjelder ansvaret for to omtvistede transaksjoner.

Klagen er sendt inn til Finansklagenemnda av foretaket.

Klager bestrider å være ansvarlig for to transaksjoner datert 7.9.20. Deler av transaksjonene lyktes banken å tilbakeføre, og det omtvistede restbeløpet utgjør nå til sammen kr 228 012. Den ene transaksjonen er en ordinær nettbanktransaksjon til en konto i Sbanken, mens den andre transaksjonen er utført ved bruk av e-Faktura til en konto i Sparebank 1 Nord-Norge. Begge kontoene tilhører tilsynelatende firmaet Pedro West – et firma som også har blitt skadelidende i denne saken.

De omtvistede transaksjonene er autorisert ved bruk av klagers personlige BankID. Det forelå ingen sikkerhetsbrudd i bankens eller Storebrands systemer i det aktuelle tidsrommet svindelen fant sted. Klager forklarer at han mottok en sms torsdag 3.9.20 kl. 19.23 fra det han trodde var Storebrand Bank ASA. Sms'en la seg på samme meldingstråd som andre sms'er klager hadde mottatt fra banken. I sms'en ble klager informert om nye pålagte sikkerhetskrav for Storebrand, og at klager straks ville motta en sikkerhetskode for sterk kundeautentisering. Klager mottok en firesifret kode, og kort tid etter ble klager oppringt fra en person som utga seg for å være ansatt i Storebrand Bank ASA sin kryptoavdeling. Personen ba om bekreftelse på mottatt kode, og klager oppga denne. Etter samtalen forklarer klager at han mottok flere telefonanrop fra ukjent nummer, samt en ny sms fra Storebrand Bank ASA kl. 19.44, hvor det stod følgende:

Registrer enheten på Michaelas iPhone. Mobilbank blir nå aktivert på din enhet. Er det ikke deg, kontakt banken umiddelbart. Koden må ikke deles med andre.

Etter dette tok klager kontakt med Storebrand Bank ASA via meldingstjenesten i nettbanken, hvor han opplyste at han mistenkte å være utsatt for svindel, samt at han ikke svarte på oppringningene fra privat nummer eller tastet flere koder som han ble tilsendt på sms.

Mandag 7.9.20 kl. 06.16 og 06.41 ble de to omtvistede transaksjonene gjennomført, og kl. 10.31 samme dag svarte banken på klagers henvendelse av 3.9.20 i meldingstjenesten i nettbanken. Banken svarte at dette hørtes ut som et svindelforsøk, men at klager – på bakgrunn av sin beskrivelse av hendelsesforløpet – ikke behøvde å være redd for at noen kunne ha fått nok informasjon til å misbruke klagers konti via nettbanken. Banken opplyste også om at de ville ta saken videre til dens sikkerhetsavdeling, og at dersom klager har klikket på lenker eller oppgitt passord eller annen sikkerhetsinformasjon, så burde klager ta kontakt med banken på nytt slik at den kan endre sms-pålogging eller passord til BankID.

Svindelen ble avdekket ved at banken ringte klager ca. kl. 14.00 samme dag for å høre om klager hadde initiert noen transaksjoner denne dagen, hvor klager besvarte bankens henvendelse negativt.

Klager anfører prinsipalt at han ikke har samtykket til transaksjonene, jf. finansavtaleloven § 24 annet ledd. Klager anfører at han ikke har utlevert noen andre engangskoder eller annen sikkerhetsinformasjon enn den ene engangskoden han mottok uoppfordret på sms fra banken den 3.9.20. Klager viser til at den eneste samhandlingen med svindlerne fant sted 3.9.20, og at han ikke gjennomførte noen handlinger på transaksjonstidspunktet 7.9.20. Videre peker klager på at han fikk varsel om at mobilbank ble etablert på "Michaelas iPhone", og at det derfor fra dette tidspunktet var tvilsomt om det fortsatt var behov for at han selv måtte autorisere transaksjonene da svindleren med stor sannsynlighet kunne gjennomføre dem via nettbanken på egenhånd. Klager viser blant annet til FinKN 2021-30 og 2020-703, hvor nemnda kom til at klager kunne holdes ansvarlig for kr 12 000. I begge sakene ble kunden forledet til å oppgi passord til BankID og engangskoder til en person som utga seg for å være fra banken, og hvor det ikke ble diskutert hvorvidt klager selv hadde autorisert transaksjonene.

Klager mener bankens anførsel om at han forsettlig har oppgitt sine personlige sikkerhetsanordninger, fremstår spekulativt og grunnløst. Klager viser til at forsett er en skyldform som foreligger når en person bevisst har utført en handling, eller når han har hatt vilje til, eller ønske om, å foreta en slik handling. Han mener det ikke foreligger holdepunkter for å legge dette til grunn, all den tid konsekvensen av at han "mislyktes i å beskytte de personlige sikkerhetsanordningene" var at det ble foretatt vesentlige transaksjoner ut fra egne konti. Det må også vektlegges at klager varslet banken umiddelbart etter at mistanken om svindel ble avdekket – noe klager mener illustrerer verken et bevisst brudd på avtale om BankID eller et ønske om eller vilje til å krenke vilkårene for BankID. Til støtte for sitt syn om at han ikke forsettlig har oppgitt sine personlige sikkerhetsanordninger, viser klager også til blant annet FinKN 2021-30 og 2020-703, hvor banken ikke fikk medhold i at klager forsettlig hadde brutt sine forpliktelser etter finansavtaleloven § 34 første ledd, jf. § 35 tredje ledd, og FinKN 2019-986 – hvor kortholder med viten og vilje hadde gitt en butikkansatt sitt betalingskort og PIN-koden til dette, hvoretter betalingsinstrumentet ble misbrukt.

Klager anfører at det i høyden er et spørsmål om han har opptrådt uaktsomt, og således om han kan holdes ansvarlig for enten kr 1 200 eller kr 12 000, jf. finansavtaleloven § 35 andre og tredje ledd. Klager erkjenner at nemndspraksis isolert sett kan tilsi at han har opptrådt grovt uaktsomt. Imidlertid viser klager til at han helt uoppfordret mottok en henvendelse fra Storebrand

Bank ASA, som la seg på samme meldingstråd som øvrige sms'er fra banken, og at han kort tid deretter ble oppringt av en person som utga seg for å være fra banken. Følgelig har han ikke opptrådt noe vesentlig annerledes enn hva en normalt aktsom person i tilsvarende situasjon ville gjort. Dette er således en helt annen situasjon enn der en person mottar eksempelvis en e-post fra Apple, hvor det normalt kan avdekkes relativt enkelt at det ikke er Apple som er avsender. Klager viser også til at han tok kontakt med banken med en gang han mistenkte svindel, og at dette må oppfattes som en formildende omstendighet. I tillegg mener klager det er altfor strengt at han burde ha reagert på at svindleren i telefonen sa han jobbet i bankens kryptoavdeling, gitt de ovennevnte omstendighetene. Klager mener han ikke kan forventes å ha inngående kjennskap til alle driftsområdene til et konsern som Storebrand.

Uavhengig av det ovennevnte, viser klager til at han varslet banken før transaksjonene ble gjennomført, og at han følgelig ikke kan holdes ansvarlig for tapet, jf. finansavtaleloven § 35 fjerde ledd. Klager mener banken hadde alle forutsetninger for å avverge tapet, uten at dette ble gjort, og at dette er noe banken må bære risikoen for.

Finansforetaket anfører prinsipalt at klager selv har samtykket til transaksjonene, jf. finansavtaleloven § 24 og § 35 første ledd, og således at han må bære tapet selv. Banken viser til at samtykket ble gitt gjennom en autorisasjonsprosedyre ved bruk av sikkerhetskoder. Til støtte for sin anførsel, viser banken til FinKN 2020-227, hvor kunden ved å utlevere sikkerhetskoder til en svindler ble ansett å ha samtykket til transaksjonene overfor banken, selv om han ble narret til det av svindleren.

Subsidiært anfører banken at klager holdes ansvarlig for hele det omtvistede beløpet fordi han forsettlig har unnlatt å oppfylle sine forpliktelser etter finansavtaleloven § 34 første ledd og § 35 femte ledd, samt mobilbankvilkårene pkt. 5. Banken viser til at klager i løpet av telefonsamtalen med svindleren ved flere anledninger har røpet sitt personlige passord og engangskoder, samt at klager har valgt å ignorere flere varsler fra banken som kunne ha forhindret svindelen. Klager har følgelig ikke tatt rimelige forholdsregler for å beskytte sine personlige sikkerhetsanordninger. Banken viser til at det er uten betydning for forsettsvurderingen om klager forstod at handlingen kunne medføre et økonomisk tap, jf. ordlyden i finansavtaleloven § 35 og prop. 92 L 2019-2020 s. 186. Banken viser også til FinKN 2019-986 som støtte for sin anførsel om at nemnda tidligere har lagt til grunn at å oppgi sikkerhetsopplysninger til andre personer er å anse som forsettlig brudd på pliktene i finansavtaleloven § 34.

Atter subsidiært anfører banken at klager har opptrådt grovt uaktsomt, og at han således kan holdes ansvarlig for kr 12 000, jf. finansavtaleloven § 35 tredje ledd. Banken viser til at klager har oppgitt sitt personlige passord og flere engangskoder til en person som sa han jobbet i bankens kryptoavdeling. Banken mener klager burde visst at Storebrand ikke driver med kryptovaluta. I tillegg vises det til at klager har fått flere varslinger fra banken forut for etableringen av mobilbank på svindlerens mobil og forut for transaksjonene, men at han ignorerte disse og i stedet valgte å utlevere engangskoder og personlig passord. Banken mener det ikke foreligger noen formildende omstendigheter.

Finansklagenemnda Banks begrunnelse

Nemnda forstår det slik at det er enighet mellom partene om at de to omtvistede transaksjonene er gjennomført som ledd i svindel rettet mot klagerens konto i banken. Banken mener likevel at transaksjonene er autorisert av klageren ved at han er blitt lurt til å gjennomføre ordinære autorisasjonsprosedyrer, slik at bestemmelsen om bankens ansvar i finansavtalel. § 35 første ledd ikke kommer til anvendelse. Subsidiært mener banken at klageren forsettlig har unnlatt å beskytte sine sikkerhetsanordninger, med det resultat at han er fullt ansvarlig etter finansavtalel. § 35

tredje ledd tredje punktum. Atter subsidiært hevder banken ansvar for egenandel på kr 12 000 for grov uaktsomhet etter § 35 tredje ledd andre punktum.

Nemnda finner faktum i saken uklart. Uklarheten gjelder selve hendelsesforløpet og måten svindelen er gjennomført på. Det er avgjørende for en konklusjon om partenes ansvar at svindelmetoden er tilstrekkelig klargjort. Klageren forklarer at den eneste opplysningen han har gitt til svindlerne, er den koden han mottok på sms 3.9. Koden kom tilsynelatende fra banken, men banken avviser å ha sendt denne. Det er uklart hva slags kode dette var, og hva den kunne brukes til som ledd i svindelen dersom den ikke kom fra banken. Banken synes å mene at den koden klageren oppga i første omgang, var klagerens vanlige PIN-kode til nettbanken, noe klageren avviser. Det er heller ikke klart for nemnda om banken mener at klageren må ha gitt BankID-opplysninger til svindlerne etter den 3.9., herunder den 7.9. da transaksjonene ble gjennomført, og på hvilken måte opplysningene i tilfelle ble gitt. Det synes uomtvistet at klageren om kvelden 3.9. gjennom nettbanken sendte melding til banken om mulig svindel. Selv om denne meldingstjenesten ikke passer på hastemeldinger som dette, setter nettbankmeldingen forklaringen om at klageren skal ha fortsatt å la seg svindle, i et merkelig lys. Det er også uklarhet omkring varsel til klageren 3.9. om at mobilbank var blitt etablert på en ny enhet.

Bankens teori om hendelsesforløpet forutsetter at klageren har oppgitt sin vanlige PIN-kode til mobilbanken til svindlerne, og at han senere har tastet eller oppgitt engangskoder flere ganger. Klageren benekter å ha gjort det. Klageren har en annen teori, som tar utgangspunkt i at svindlerne lyktes i å skaffe seg tilgang til klagerens mobilbank, og på den måten har kunnet gjennomføre transaksjoner flere dager etter at svindelen startet.

Det følger av vedtektene for Finansklagenemnda pkt. 4.1 bokstav d) at en sak kan avvises fra nemndsbehandling dersom "saken ikke lar seg behandle uten at dette i særlig grad går utover klageorganets effektivitet". Denne avvisningsregelen svarer til lov om godkjenning av klageorganer for forbrukersaker § 14 første ledd bokstav f). I forarbeidene til loven er det i Prop. 32 L (2015-2016) under pkt. 10.6.1.3 forutsatt at avvisningsregelen kan benyttes "der klageorganet ikke anser tvisten å være egnet for deres behandling, for eksempel på grunn av bevissspørsmål". Slik bevisituasjonen er i denne saken, finner nemnda at saken må avvises i medhold av vedtektene pkt. 4.1 bokstav d).

Når en kunde bestrider å ha ansvar for en uautorisert betalingstransaksjon etter finansavtalel. § 35, skal banken ifølge § 37 første ledd tilbakeføre beløpet til kontoen. Unntak fra dette gjelder etter § 37 andre ledd bokstav b) dersom banken innen fire uker fra mottakelse av skriftlig innsigelse har anlagt søksmål mot kunden eller brakt saken inn for Finansklagenemnda. Dersom saken blir avvist fra nemnda, løper det ifølge § 37 tredje ledd ny frist på fire uker for banken til å tilbakeføre beløpet eller ta ut søksmål mot kunden. Nemnda ser det slik at regelen i § 37 tredje ledd kommer til anvendelse selv om det i denne saken var kunden, og ikke banken, som brakte saken inn for Finansklagenemnda.

Avgjørelsen er enstemmig.

Finansklagenemnda Banks konklusjon

Saken avvises fra behandling ved Finansklagenemnda.

Ved behandlingen deltok Trygve Bergsåker (leder), Knut Bjerve (selskapsrepresentant) og Kristoffer Sørli (forbrukerrepresentant).