

# Finansklagenemnda Bank

## Avgjørelse FinKN 2023-537

5.7.2023

### Vipps Mobilepay AS

### Betalingsformidling

Phishing – tekstmelding før oppringning.

Kontohaver mottok en tekstmelding med lenke som tilsynelatende var fra Kredinor. Kontohaver klikket på lenken og la inn sitt fødselsnummer. Hun ble deretter oppringt av noen som utga seg for å være fra Sparebank1. Vedkommende sa at kontohaver var utsatt for svindel, og at han skulle hjelpe kontohaver med å sperre BankID og kort. Kontohaver fikk tilsendt koder til sin telefon som hun godkjente. Det ble opprettet en ny mobilenhet på kontohavers Vippsprofil og utført to transaksjoner fra kontohavers konto. Foretaket holdt kontohaver ansvarlig for kr 12 000. Nemnda kom til at det ikke var grunnlag for å holde kortholder ansvarlig. Kortholder fikk medhold.

ANTATT ØKONOMISK OMFANG: kr 12 000

---

### Saksfremstilling

Saken gjelder to transaksjoner på til sammen kr 98 000. Foretaket holder kontohaver ansvarlig for kr 12 000.

Kontohaver mottok 22.11.22 kl. 16.16 følgende tekstmelding fra telefonnummeret +47 XXX:

Vi har sendt et eller flere brev til din postkasse på Min side. Du kan logge deg inn via lenken nedenfor.  
Vennlig hilsen Kredinor AS.

One or mor letters is available in your mailbox at My page. To view the letter, click on the link bellow.  
Best regards Kredinor AS.

<https://dev-altinn-m-side.pantheonsite.io>

Kontohaver har forklart at hun trykket på lenken i tekstmeldingen og la inn sitt fødselsnummer.

Kontohaver ble deretter oppringt av noen som utga seg for å være fra Sparebank1. Vedkommende sa at kontohaver var utsatt for svindel, og at han skulle hjelpe henne med å sperre BankID og kort. Kontohaver bestrider å ha oppgitt passord over telefon, men bekrefter å ha godtatt koder hun fikk tilsendt til sin telefon.

Foretaket har opplyst at det ble registrert en ny mobilenhet på kontohavers Vippsprofil kl. 17.05. Dette muliggjorde at svindleren kunne gjennomføre to transaksjoner rundt kl. 17.50 på til sammen kr 98 000 (+ kr 980 i gebyr). Kontohavers BankID på mobil er benyttet til å verifisere registrering av ny mobilenhet i Vipps og ved begge transaksjonene.

Foretaket anser det sannsynliggjort at kontohaver er svindlet, men holder henne ansvarlig for en egenandel på kr 12 000.

**Kontohaver** har anført at hun ikke har opptrådt grovt uaktsomt. Kontohaver var på jobb med ansvar for en pasient da hun mottok e-posten og ble oppringt. Hun ble stresset. Kontohaver har bestridt at hun oppga passord over telefonen og skjønnte ikke at svindleren var kommet inn i nettbanken hennes.

**Finansforetaket** har anført at kontohaver har handlet grovt uaktsomt.

### **Finansklagenemnda Banks begrunnelse**

Partene er enige om at kontohaveren er blitt svindlet. Foretaket mener at kontohaveren kan holdes ansvarlig for en egenandel på kr 12 000 etter finansavtalel. § 35 tredje ledd andre punktum, jf. § 34 første ledd, for grovt uaktsomt å ha unnlatt å beskytte sikkerhetsanordningene knyttet til sin BankID.

Som ledd i svindelen ble det opprettet en ny mobilenhet på kontohaverens profil. Både opprettelsen av den nye enheten og de to omtvistede betalingstransaksjonene ble bekreftet med kontohaverens BankID på mobil. Kontohaveren forklarer at hun godtok koder som hun fikk tilsendt på sin mobiltelefon. Det avgjørende spørsmålet i saken er om det var grovt uaktsomt av henne å gjøre dette.

Det er generelt grunn til årvåkenhet mot uventede tekstmeldinger med lenker. At den tekstmeldingen som kontohaveren mottok, kom fra et vanlig telefonnummer, var egnet til å vekke mistanke. Det samme var teksten på lenken ([dev-altinn-m-side.pantheonsite.io](http://dev-altinn-m-side.pantheonsite.io)). Innholdet i meldingen var derimot ikke spesielt lite troverdig. Kontohaveren åpnet lenken på tekstmeldingen og oppga sitt fødselsnummer. Dette ga svindleren grunnlag for å starte opprettelse av ny enhet tilknyttet kontohaverens profil. Kontohaveren ble deretter oppringt av svindleren, som oppga å være fra en bank, og som skulle hjelpe henne med å forhindre en svindel som hun var utsatt for. Kontohaveren godkjente så opprettelsen av ny enhet og de to betalingene ved å godta koder som hun mottok på sin telefon. Hun gjorde dette i tillit til samtalen med den angivelige bankpersonen, for å unngå svindel rettet mot seg.

Slik hendelsesforløpet er beskrevet i saken, vurderer nemnda saken slik at kontohaverens opptreden var uaktsom, men ikke grovt uaktsom, slik loven krever for egenandel på kr 12 000.

Lovens regel om egenandel på kr 12 000 ved grov uaktsomhet finnes også i foretakets kundevilkår. Uten at det er av betydning i saken, vil nemnda bemerke at kundevilkårene har fått en tvetydig utforming i pkt. 6.5. I andre avsnitt finnes først en bestemmelse om egenandel på kr 12 000 ved grov uaktsomhet. Deretter heter det at kunden er fullt ansvarlig for tapet dersom han eller hun ved forsett eller grov uaktsomhet har unnlatt å oppfylle sine forpliktelser i avtalen. Finansavtaleloven av 1999 § 35 tredje ledd gir ikke adgang til å pålegge kunden fullt ansvar for grov uaktsomhet dersom den uautoriserte betalingstransaksjonen er gjort med elektronisk betalingsinstrument.

Avgjørelsen er enstemmig.

### **Finansklagenemnda Banks konklusjon**

Kontohaveren gis medhold.

*Ved behandlingen deltok Trygve Bergsåker (leder), Tom Slungaard (selskapsrepresentant) og Kristoffer Sørлие (forbrukerrepresentant).*