NOTAT

FNO
Finansnæringens Fellesorganisasjon

***Aktørenes navn er endret***

**Tvist for Ansvarsregulerende utvalg – sak 2/11**

# Mellom
# Lillevik Privatbank og Storevik Bank

# Spørsmål om erstatningsansvar etter misbruk av en kompromittert PersonBankID

Behandlet av Ansvarsregulerende utvalg i møte 26. august 2011.

Lillevik Privatbank har ved brev 8. mars 2011 til sekretariatet for Ansvarsregulerende utvalg (AU) oversendt en tvist med Storevik Bank med anmodning om behandling og avgjørelse av saken.

Saken gjelder i korthet spørsmålet om Storevik Bank kan holdes erstatningsansvarlig for det tap som er påført Lillevik Privatbank som følge av urettmessig belastning av konto i banken etter misbruk av PersonBankID utstedt av Storevik Bank.

Lillevik Privatbank har prinsipalt nedlagt påstand om at Storevik Bank skal erstatte Lillevik Privatbank kr 343.946,26, subsidiært kr 100.000,-.

Storevik Bank har prinsipalt nedlagt påstand om frifinnelse, subsidiært at ansvaret begrenses til kr 100.000,-.

## 1. Sakens aktører

Lillevik Privatbank – klager
Storevik Bank – innklaget
Marit Molander – kunde i Lillevik Privatbank og Storevik Bank

## 2. Dokumenter i saken mv

Følgende dokumenter forelå for Ansvarsregulerende utvalg ved behandlingen av saken:

a) Lillevik Privatbanks brev 8. mars 2011 til AU med vedlegg 1-8
b) Storevik Banks brev 4. april 2011 til AU
c) Lillevik Privatbanks brev 19. april 2011 til AU med vedlegg 9-11
d) Storevik Banks brev 9. mai 2011 til AU
e) Regler om BankID, senest endret 29. oktober 2010.
f) Samlet kravdokument for sikkerhet i BankID, versjon 1.1, fastsatt av BSK 14. juni 2010.

**3. Sakens faktum**

Molander etablerte 13. september 2010 et kundeforhold i Storevik Bank. Kundeforholdet omfattet brukskonto, betalingskort m/ VISA og Bankkort med bilde, nettbank og PersonBankID. Molander fikk tilsendt BankID passord på SMS 22. september mens OTP-mekanismen (sikkerhetskortet) ble utsendt pr manuell post 27. september.

Den 5. oktober mottar Storevik Bank en elektronisk forespørsel om å sende nytt BankID-passord til Molanders folkeregistrerte adresse.

7. oktober tar Molander kontakt med Storevik Bank og påpeker at hun ikke har mottatt betalingskort, OTP og annet nødvendig sikkerhetsutstyr fra Storevik Bank. Kunden purrer på nytt 12. oktober. Molander henvender seg igjen til Storevik Bank 14. oktober. Storevik Bank sjekker da status på den nyopprettede brukskontoen og oppdager at kontoen er overtrukket uten at Molander har foretatt innskudd eller annen bruk av kontoen. Storevik Bank sperrer samme dag (14. oktober) BankID, kontoen og tilhørende betalingskort.

Molander politianmelder forholdet som tyveri 15. oktober.

Molander hadde fra tidligere et kundeforhold i Lillevik Privatbank i form av en sparekonto (uten betalingskort). To dager før Storevik Bank sperret BankID'en, dvs. 12. oktober, har uvedkommende benyttet den Storevik Bank-utstedte BankID'en til å bestille et VISA-kort tilknyttet Molanders sparekonto i Lillevik Privatbank. VISA-kortet og tilhørende PIN-kode var sendt pr. post til Molanders folkeregisterte adresse. Det antas at kort og PIN er plukket opp og frastjålet fra Molanders postkasse tilsvarende som forsendelsene fra Storevik Bank.

Den 26. oktober sjekker Molander sin sparekonto i Lillevik Privatbank og oppdager urettmessige belastninger (uautoriserte transaksjoner) på kontoen. Molander henvender seg til Lillevik Privatbank og får sperret sparekontoen og VISA-kortet umiddelbart.

Molanders sparekonto i Lillevik Privatbank belastes urettmessig for til sammen kr. 343.946,26 i tidsrommet 18. oktober til 26. oktober.

**4. Partenes anførsler og krav**

*4.1 Lillevik Privatbank*
Lillevik Privatbank anfører at Storevik Bank har handlet erstatningsbetingende uaktsomt ved å ha gjort det mulig for uvedkommende å bestille et VISA-kort tilknyttet kundens sparekonto i Lillevik Privatbank for deretter urettmessig å belaste sparekontoen for til sammen kr. 343.946,26 i tidsrommet 18. oktober til 26. oktober. Lillevik Privatbank viser bl.a. til Regler om BankID pkt. 15, jfr. pkt. 12.

Lillevik Privatbank har prinsipalt nedlagt påstand om at Storevik Bank skal erstatte Lillevik Privatbank kr 343.946,26, subsidiært kr 100.000,-.

*4.2 Storevik Bank*
Storevik Bank fremholder at banken ikke var noe å bebreide for at Molanders BankID ikke ble sperret før 14. oktober, at BankID'en urettmessig ble benyttet for å bestille et VISA-kort tilknyttet kundens sparekonto i Lillevik Privatbank eller at banken på annen måte har opptrådt erstatningsansvarlig.

Storevik Bank har prinsipalt nedlagt påstand om frifinnelse, subsidiært at ansvaret begrenses til kr 100.000,-.

**5. Ansvarsregulerende utvalgs vurderinger**

*5.1 Problemstillingen – relevant regelverk*
Ansvarsregulerende utvalg legger til grunn at den PersonBankID som Storevik Bank hadde utstedt til Molander ble benyttet av uvedkommende til å bestille et VISA-kort tilknyttet Molanders sparekonto i Lillevik Privatbank. Ved bruk av dette VISA-kortet ble Molanders sparekonto i Lillevik Privatbank urettmessig belastet for til sammen kr. 343.946,26 i tidsrommet 18. oktober til 26. oktober.

Det rettslige spørsmålet som Ansvarsregulerende utvalg skal ta stilling til i denne saken, er om Storevik Bank i tidsrommet fra utstedelsen av BankID'en til sperringen ble gjennomført 14. oktober, opptrådte erstatningsbetingende uaktsomt med den følge at uvedkommende kunne misbruke BankID'en for bestilling av VISA-kortet i Lillevik Privatbank to dager i forveien, dvs. 12. oktober. Dersom utvalget finner at Storevik Bank handlet uaktsomt, vil banken kunne være erstatningsansvarlig for hele eller deler av det økonomiske tapet som

ble påført Lillevik Privatbank som følge av de urettmessige belastningstransaksjonene på Molanders sparekontoen i Lillevik Privatbank.

Utvalget vil anvende Regler om BankID på saksforholdet. Reglene ble senest endret av Bransjestyre bank og betalingsformidling (FNO) 29. oktober 2010, men disse endringene har ingen betydning for tvisten mellom Lillevik Privatbank og Storevik Bank.

Med hjemmel i Regler om BankID pkt. 3, jfr. pkt. 21, har Bankenes Standardiseringskontor (BSK) den 14. juni 2010 fastsatt" Samlet kravdokument for sikkerhet i BankID". Disse sikkerhetskravene kommer etter utvalgets mening til anvendelse på forholdet.

*5.2 Var utstedelsen av passord og OTP-mekanismen tilfredsstillende?*
Første forhold som må vurderes er om Storevik Bank fulgte de sikkerhetskrav som er fastsatt for utsendelse av BankID passord og OTP-mekanismer til sluttbruker, dvs. Molander. Etter Regler om BankID pkt 15 første ledd vil utstederbanken kunne bli erstatningsansvarlig for annen banks tap, dersom utstederbanken har handlet uaktsomt i forbindelse med utstedelsen av BankID, herunder om passord og OTP-mekanisme (sikkerhetskortet) ble distribuert korrekt.

BSK har i" Samlet kravdokument for sikkerhet i BankID" pkt 7.1 fastsatt krav til alternative utsendelsesmåter (i én sikker kanal eller to kanaler). Storevik Bank sendte Molander BankID passord på SMS 22. september mens OTP-mekanismen (sikkerhetskortet) ble utsendt ved manuell post 27. september. En slik utsendelsesprosedyre i to kanaler synes å være i overensstemmelse med disse kravene pkt. 7.1.2 og 7.1.4.

Den 5. oktober sender Storevik Bank på nytt ut BankID passord på grunnlag av en elektronisk forespørsel (tilsynelatende fra Molander). Denne gang ble passordet sendt pr ordinær post til Molanders folkeregistrerte adresse. Bruk av en ny kanal for utsendelse av nytt BankID passord er etter utvalgets i overensstemmelse med" Samlet kravdokument for sikkerhet i BankID" pkt. 7.2.3, men det stilles samtidig krav om at dersom én komponent skal nyutsendes uten at banken har autentisert kunden på nytt, skal det i tillegg til selve utsendelsen gis melding til sluttbrukeren om at forsendelsen er på vei. Sistnevnte forhold er ikke omtalt i partenes saksdokumenter, men utvalget kan ikke utelukke at Storevik Bank i sitt svar på den elektroniske forespørselen har gitt beskjed om at nytt passord var på vei.

Selv om uvedkommende, trolig etter tyveri av post fra Molanders postkasse, har klart å få tilgang til både BankID passord og OTP-mekanisme, kan utvalget ikke se at Storevik Banks utsendelsesrutiner avvek fra" Samlet kravdokument for sikkerhet i BankID".

*5.3 Burde Storevik Bank sperret sertifikatet på et tidligere tidspunkt?*
I Regler om BankID pkt. 12 er det inntatt krav til utstederbanken om å sperre (suspendere/tilbakekalle) et BankID dersom det" er eller kan forventes å bli misbrukt". Uaktsom overtredelse av denne sperreplikten vil kunne medføre erstatningsansvar for utstederbanken dersom andre banker lider tap ved å ha stolt på et BankID som burde ha vært sperret, jfr. ansvarsbestemmelsen i Regler om BankID pkt. 15.

BSK har i sin sertifikatpolicy for banklagret BankID pkt. 4.4 (sperring av sertifikater) listet opp noen eksempler på forhold som skal lede til tilbakekall av et BankID:

- uautorisert eller mistenkt uautorisert tilgang til private nøkler,
- kompromittering eller tyveri av aktiveringsdata,
- kjent misbruk av et sertifikat,
- sertifikatholder har skiftet navn,
- sertifikatholder er ikke lenger berettiget til å ha sertifikatet,
- opphør av sertifikatholders kundeforhold til banken.

For å sperre en BankID kan banken velge enten å tilbakekalle den permanent eller la det først være suspendert. Det vil generelt stilles svakere krav til visshet og til dialogen med sertifikatholder for å iverksette en tidsbegrenset suspendering enn for å tilbakekalle et sertifikat.

Lillevik Privatbank stolte på en positiv valideringsforespørsel 12. oktober i forbindelse med bestillingen av VISA-kortet som senere ble misbrukt i perioden 18. oktober til 26. oktober. Storevik Bank sperret BankID'en den 14. oktober, men spørsmålet er om Storevik Bank allerede 7. eller 12. oktober, ved Molanders etterlysing av forsendelsen av bl.a. OTP-mekanismen, burde ha undersøkt forholdet nærmere for å kunne vurdere om det forelå en risiko for at sikkerhetsmekanismene hadde kommet bort eller frastjålet og at BankID'en kunne forventes å bli misbrukt.

OTP-mekanismen mv ble utsendt pr post mandag 27. september. Normal forsendelsestid av B-post er 3 til 5 virkedager i Norge. Når Molander tar kontakt med Storevik Bank torsdag 7. oktober for å etterlyse forsendelsen, er det gått over 10 dager siden utsendelsen. Storevik Bank fant derimot ikke grunnlag for å sperre BankID'en, med henvisning til at det ikke er unormalt med forsinkelser i postgangen. Ansvarsregulerende utvalg avviser ikke at

det forekommer forsinkelser i postgangen, men etter 10 dager burde banken ha reagert med tiltak for å begrense eller hindre mulige tap og andre skadevirkninger i tilfellet passordet og OTP-mekanismen hadde kommet på avveier. Tyveri fra postkasser er ikke uvanlig og ID-tyveri er økende samfunnsproblem.

Som omtalt foran under pkt. 5.2, sendte Storevik Bank den 5. oktober ut et nytt BankID passord til Molanders folkeregistrerte adresse. Etter utvalgets mening burde banken ha undersøkt dette forholdet nærmere, da Molander tok kontakt med banken den 7. oktober. Banken kunne ha brakt klarhet i dette forholdet ved å spørre Molander om det egentlig var hun som hadde rekvirert det nye passordet.

Generelt skal utstederbanker etter utvalgets mening ta som utgangspunkt at dersom det er en risiko for at passord og øvrige sikkerhetsmekanismer har kommet på avveier (så som frarøvet i posten), vil det måtte forventes at BankID'en er eller vil kunne bli kompromittert. Utvalget vil i denne forbindelse vise til Regler om BankID pkt. 12 tredje avsnitt som pålegger banker å sørge for at det finnes hensiktsmessige rutiner for å motta og behandle meldinger fra egne kunder/sertifikatholdere som ønsker at BankID skal sperres. I slike saker må det forventes skjerpet aktsomhet i bankene. At suspendering eller tilbakekall må være ønsket fra kundens side, kan etter utvalgets vurdering ikke tas bokstavlig. Bankene kan ikke forvente at kunder flest har tilstrekkelig kompetanse til å vurdere behovet for at" noe" må sperres i et slikt foreliggende tilfelle. Banken må på selvstendig grunnlag selv reagere med undersøkelser og eventuell suspensjon/sperring.

Etter Ansvarsregulerende utvalgets vurdering tilsier disse forholdene at Storevik Bank den 7. oktober burde ha behandlet Molanders henvendelse (purring) som en tapsmelding og suspendert den aktuelle PersonBankID'en.

*5.4 Andre skadereduserende tiltak*
I partenes dokumenter til Ansvarsregulerende utvalg er omtalt bankenes kontaktnettverk og andre ordninger for informasjonsutveksling mellom banker, herunder sporing av kompromitterte BankID'er. Det er brakt på det rene at kontaktnettverket ikke gjelder for BankID.

Etter utvalgets vurdering ville uthenting og spredning av transaksjonsdata fra Nets kunne ha fått en skadereduserende effekt i den foreliggende sak dersom dette hadde blitt iverksatt av Storevik Bank samtidig med politianmeldelsen 15. oktober. Da ville Lillevik Privatbank kunne ha sett at den aktuelle BankID'en hadde vært misbrukt for å bestille et VISA-kort den 12. oktober. VISA-kortet kunne Lillevik Privatbank ha sperret før de

urettmessige belastningstransaksjonene fant sted i tidsrommet 18. til 26. oktober. Ordningen med sporing av BankID'er (dvs. uthenting av data fra en transaksjonslogg som føres av Nets i faktureringsøyemed) for å varsle de øvrige banker om hvor kompromitterte BankID'er har vært benyttet, er imidlertid ikke en obligatorisk rutine for bankene og har derfor ingen betydning for utfallet av denne saken.

*5.5 Erstatningsbeløpets størrelse - begrensning*
Etter utvalgets vurdering opptrådte Storevik Bank uaktsomt ved ikke å sperre BankID'en allerede 7. oktober. Etter Regler om BankID pkt. 15 første og andre avsnitt er derfor banken å anse som erstatningsansvarlig for hele eller deler av Lillevik Privatbanks økonomiske tap ved at kompromitterte PersonBankID'en ble benyttet til å bestille et VISA-kort knyttet til Molanders sparekonto i Lillevik Privatbank.

Dette VISA-kortet ble brukt til å belaste Molanders sparekonto for til sammen kr. 343.946,26 i tidsrommet 18. oktober til 26. oktober. Tapsbeløpet er sammenfallende Lillevik Privatbanks prinsipale erstatningskrav overfor Storevik Bank.

Det følger av Regler om BankID pkt. 15 fjerde avsnitt at bankens ansvar etter første og andre ledd i alle tilfeller er begrenset til kr 100.000,- for hver transaksjon. Utvalget mener at bruken av BankID'en og det tilhørende VA-oppslaget for å bestille VISA-kortet i Lillevik Privatbank, er å anse som én transaksjon. Flere transaksjoner ble ikke gjennomført med BankID'en (i denne saken). At selve VISA-kortet ble misbrukt gjentatte ganger mellom 18. og 26. oktober er ikke av betydning for å vurdere transaksjonsbegrepet etter BankID-reglene. Storevik Banks erstatningsansvar begrenses derfor oppad til kr 100.000,-.

I tillegg til erstatningsbeløpet på kr 100.000,- skal Lillevik Privatbank kompenseres for sitt rentetap etter reglene i Alminnelig regelverk om ansvarsregulering mellom banker ved betalingsformidling § 2 første avsnitt, jfr. Regler om BankID pkt. 15 sjette avsnitt.

**6. Uvalgets avgjørelse**

Ansvarsregulerende utvalg har etter dette kommet til at Storevik Bank er forpliktet til å yte Lillevik Privatbank en erstatning på kr 100.000,- med tillegg av forsinkelsesrentelovens rente fra 28. oktober 2010 til betaling skjer.

Utvalgets avgjørelse er enstemmig.

----oOo----

Følgende medlemmer og varamedlemmer deltok under behandlingen:

- Advokat Anne Ystenes, DnB NOR Bank
- Advokat Marianne Kirkeleit, Sparebanken Vest
- Fagsjef Lise Andersen, Sparebank1 Gruppen
- Advokat Torjus Moe, Handelsbanken
- Direktør Marit Solem, yA Bank (vara)
- Daglig leder Knut Kvalheim, BSK

Følgende medlemmer deltok ikke i behandlingen:

- Advokat Camilla Rieber Waldjac, Storevik Bank
- Advokat Lillian Kvitberg Angell, Lillevik Privatbank
- Advokat Gunnar Harstad, FNO (vara)